PRIMECLUSTER™

Global Link Services

Configuration and Administration Guide 4.1

Redundant Line Control Function

(Solaris™ Operating System)

Edition October 2005

Contents

Introduction

Purpose

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

Who should use this document

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

Abstract

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

Chapter 1 Overview

This chapter explains the redundant line control function of GLS.

Chapter 2 Feature description

This chapter outlines the functions and features of GLS.

Chapter 3 Environment configuration

This chapter discusses how to set up and configure GLS.

Chapter 4 Operation

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

Chapter 5 GLS operation on cluster systems

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

Chapter 6 Maintenance

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

Chapter 7 Command references

This chapter outlines GLS commands.

Appendix A Messages and corrective actions

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

Appendix B Examples of configuring system environments

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

Appendix C Changes from previous versions

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

Appendix D Notice of supplemental information

This appendix provides supplemental information regarding GLS.

Notational convention

The document conforms to the following notational conventions:

- Text that requires special attention

- Information that users should be cautious of

- Information that users can refer to

- Manuals users find workable

- Brief summary of important information that users should understand

Trademark

UNIX is a registered trademark of The Open Group in the United States and other countries.

Sun, Sun Microsystems, the Sun Logo, and Solaris, are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Ethernet is a trademark of Fuji Xerox Corporation.

PRIMECLUSTER is a registered trademark of Fujitsu Ltd.

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

Requests

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

6th Edition
October, 2005

Chapter 1 Overview

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

1.1 What is redundant line control?

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

GLS enables the following network control methods:

Fast switching mode

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

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

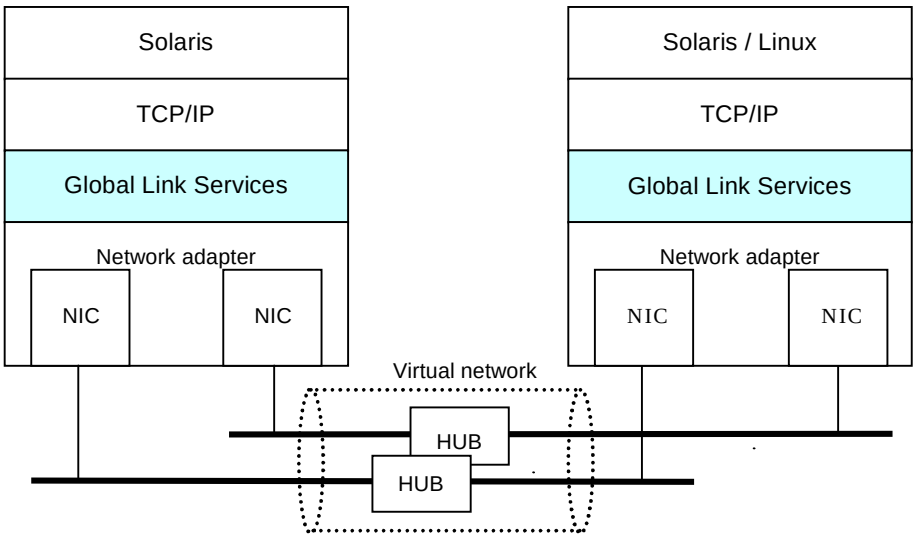


Figure 1.1 Fast switching mode

RIP mode

RIP mode enables the system to control the network line by standard TCP/IP routing protocol called Routing Information Protocol (RIP). In this mode, one of the duplex paths is used according to the RIP information. When a failure occurs, the system switches to the alternative route. The standard protocol allows communications with other remote systems and also with host systems on the other networks connected via routers. However, path switching in the RIP mode is slow and time-consuming.

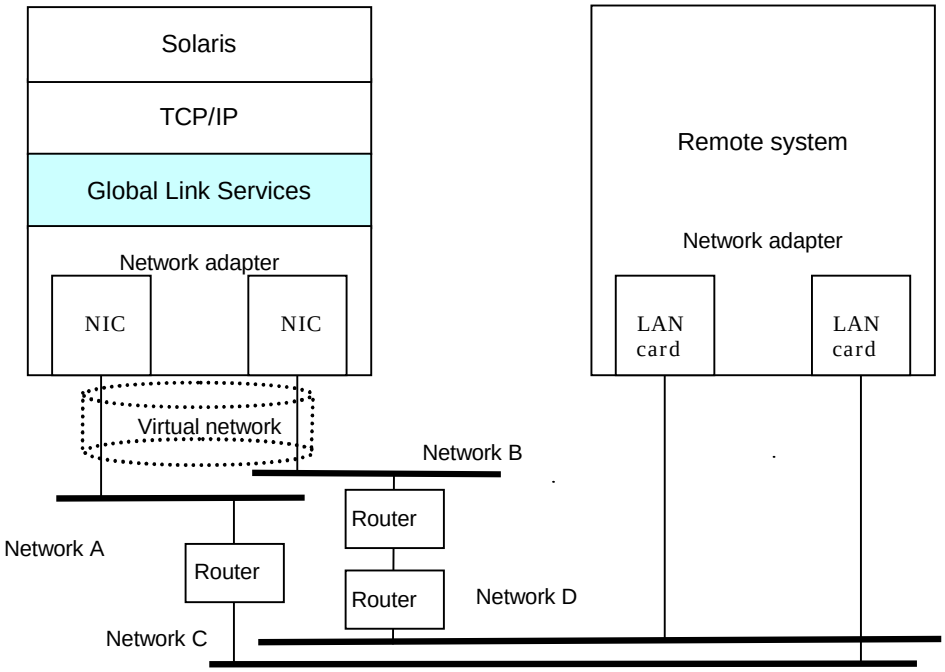


Figure 1.2 RIP mode

NIC switching mode

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

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

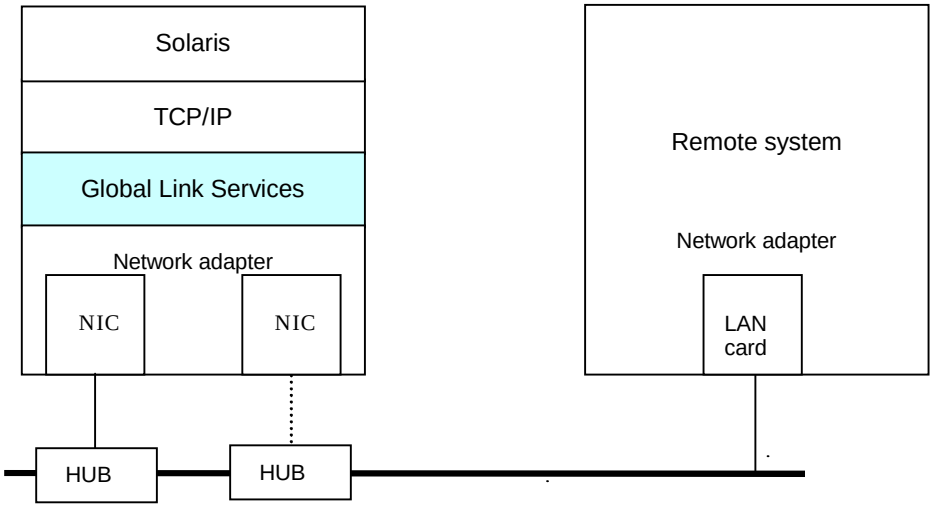


Figure 1.3 NIC switching mode

GS/SURE linkage mode

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

GS/SURE connection function

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

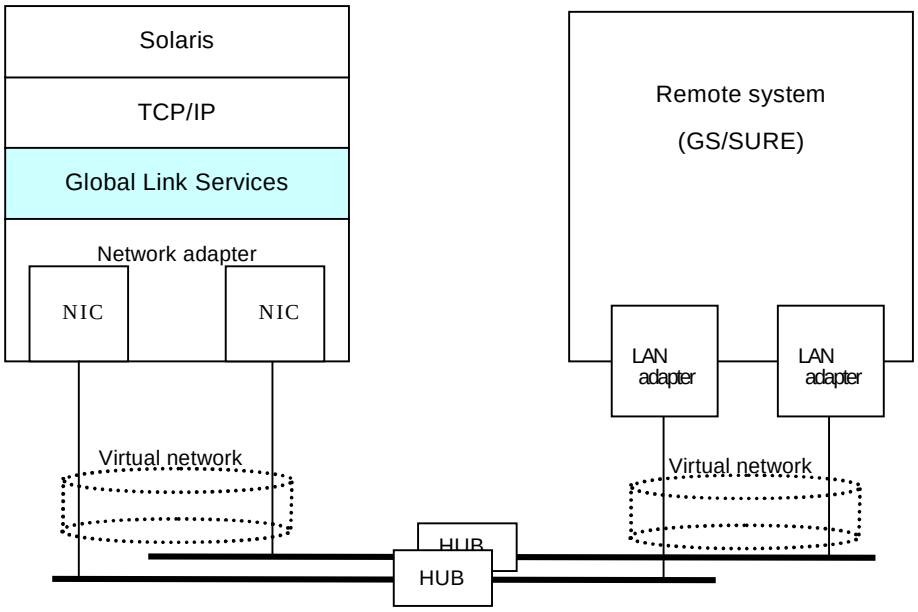


Figure 1.4 GS/SURE linkage mode (GS/SURE connection function)

TCP relay function

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

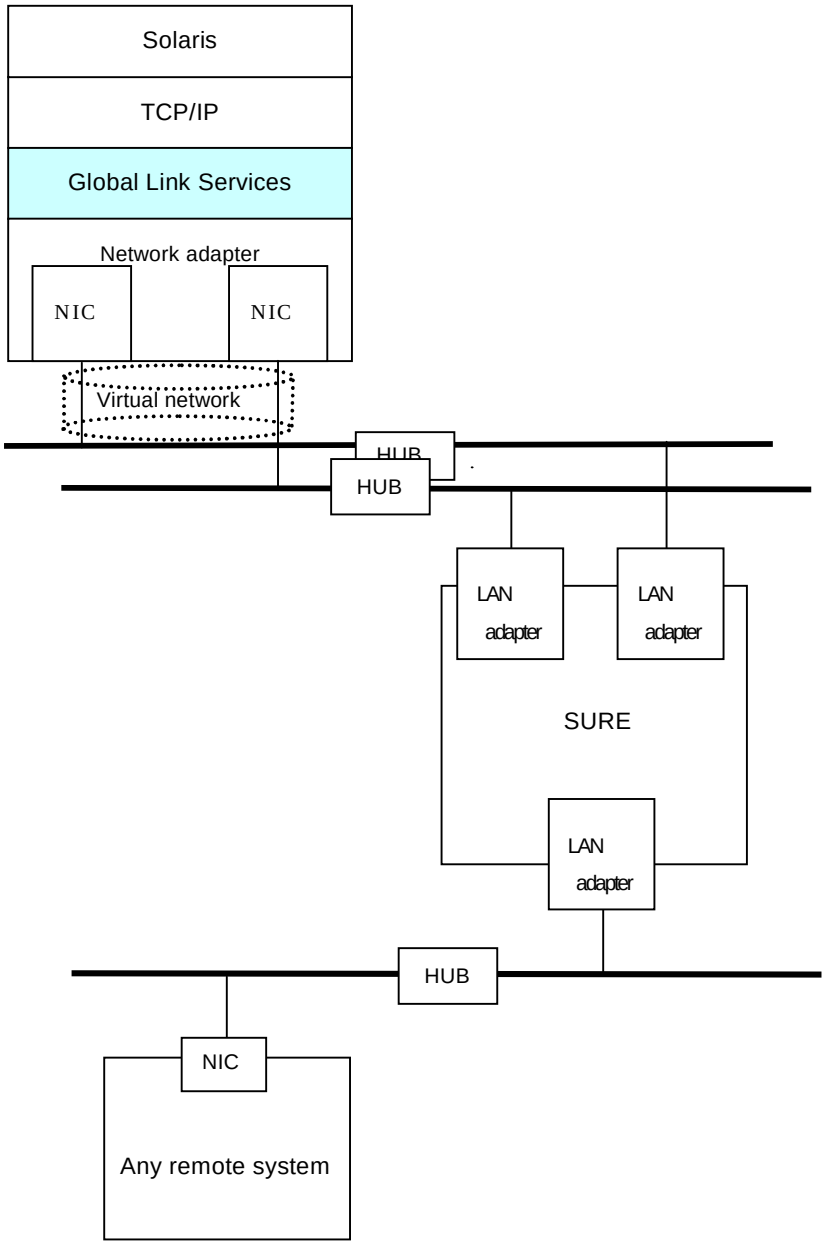


Figure 1.5 GS/SURE linkage mode (TCP relay function)

1.1.1 Functional comparison

The following table compares the functions of each network switching mode.

Table 1.1 Function comparison

Redundant line switching method			**Fast switching mode**	**RIP mode**
Network control			Makes both of redundant transmission routes active and uses them concurrently. A stream of data is sent on a TCP connection.	Makes both of redundant transmission routes active and uses either of the transmission routes according to the standard protocol, RIP Routing Information Protocol).
Fault monitoring	Detectable failures		NIC, cable, HUB, remote host	NIC, cable, HUB, router
	Fault monitoring	Monitoring method	Monitors framework between the NIC of the host and that of the remote host. If the frame communication is disrupted, a transmission route failure will be detected.	Monitors sending and receiving RIP packets. If the packet communication is disrupted, a transmission route failure will be detected.
		Failure detection time	5 to 10 seconds (Default)	5 minutes (non-tunable)
	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.	Monitors sending and receiving RIP packets. If the packet communication is disrupted, a transmission route failure will be detected.
		Recovery detection time	1 to 5 seconds (Default)	1 to 30 seconds (non-tunable)
	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.
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.	Switches a failed transmission route according to RIP packet routing.
	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 an ongoing operation according to RIP packet routing. Manual switchback is not supported.
Conditions	Remote hosts		PRIMEPOWER, GP7000F, PRIMERGY, PRIMEQUEST	Arbitrary host
	IP addresses		IPv4 address, IPv6 address	IPv4 address
	Solaris container		Operated on a global zone. Ensures a high-reliability communication infrastructure on both of the global and non-global zones.	Operated in a global zone. Ensures a high-reliability communication infrastructure on the global zone only.

Redundant line switching method			**NIC switching mode**	**GS/SURE linkage mode**
Network control			Activates and uses one redundant transmission route exclusively and deactivates the other route.	Makes both of redundant transmission routes active and uses them concurrently. A stream of data is sent on a TCP connection.
Fault monitoring	Detectable failures		NIC, cable, HUB,	NIC failure, Cable failure, HUB failure, Remote host failure (system failure)
	Fault monitoring	Monitoring method	Monitors HUB using the ping command. If the HUB communication is disrupted, a transmission route failure will be detected.	Monitors a remote host using the ping command. If the communication is disrupted, a transmission route failure will be detected.
		Failure detection time	25 to 30 seconds. (Default)	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 within a specified time, 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	About 1 to 15 seconds (Default)	About 1 to 5 seconds. (Default)
	Fault monitoring start/stop		Automatically starts along with virtual interface activation and stops along with its deactivation. Manual startup or stop of fault monitoring is also allowed with the operational command.	Automatically starts along with virtual interface activation and stops along with its deactivation. Manual startup or stop of fault monitoring is also allowed with the operational command.
Line switching	Switchover		Automatically deactivates NIC of a failed transmission route and activates a standby NIC. Manual switching operation is also allowed with the operational command.	Automatically disconnects a failed transmission route and uses the other transmission route. Manual switching operation is not supported.
	Switchback		If a failed transmission route is recovered, it will automatically rejoin operation as a standby NIC. Manual rejoining is also allowed with the operational command.	If a failed transmission route is recovered, it will automatically join communication. Manual rejoining is not supported.
Conditions	Remote hosts		Arbitrary host	GS (Global Server), SURE SYSTEM, ExINCA
	IP addresses		IPv4 address, IPv6 address	IPv4 address

	Solaris container	Operated on a global zone. Ensures a high-reliability communication infrastructure on both of the global and non-global zones.	Operated in a global zone. Ensures a high-reliability communication infrastructure on the global zone only.

1.1.2 Criteria for selecting redundant line control methods

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

The flow chart for shown in Figure 1.6 will assist in determining the redundant line control method that would be the most effective for you.

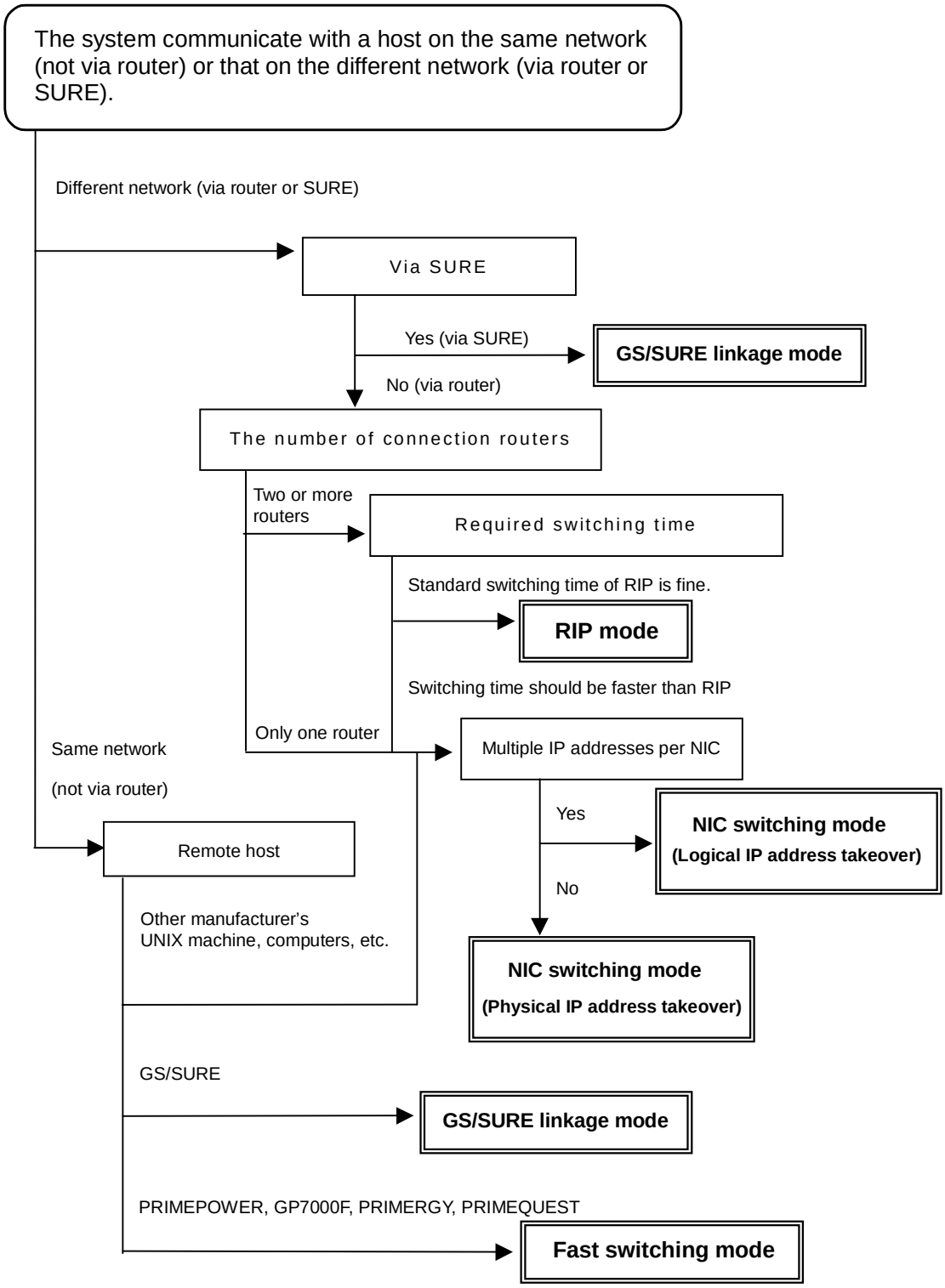


Figure 1.6 Redundant line control method decision flow chart

1.2 Redundant line control effects

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

1.3 System Configuration

Fast switching mode and RIP mode

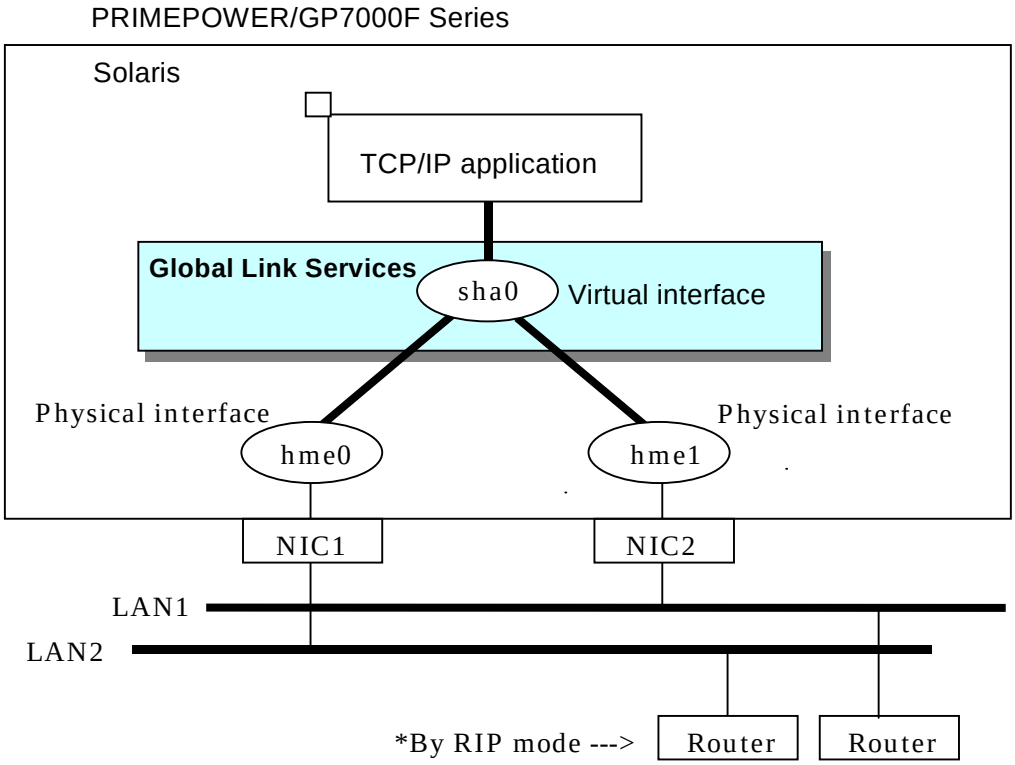


Figure 1.7 Fast switching mode and RIP mode

NIC switching mode

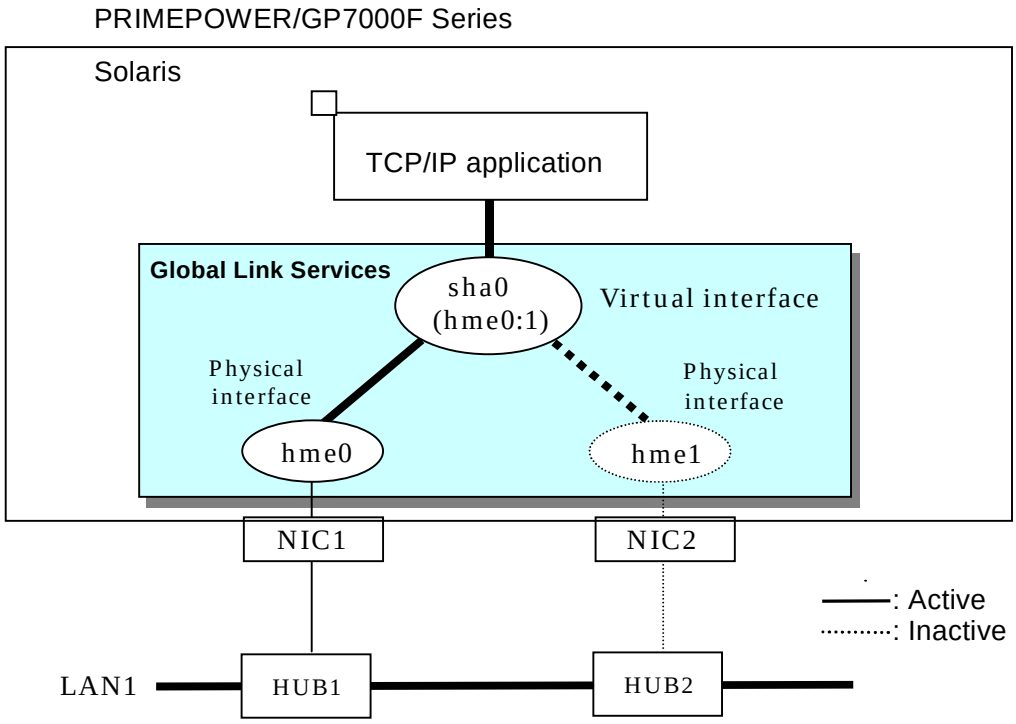


Figure 1.8 NIC switching mode

GS/SURE linkage mode

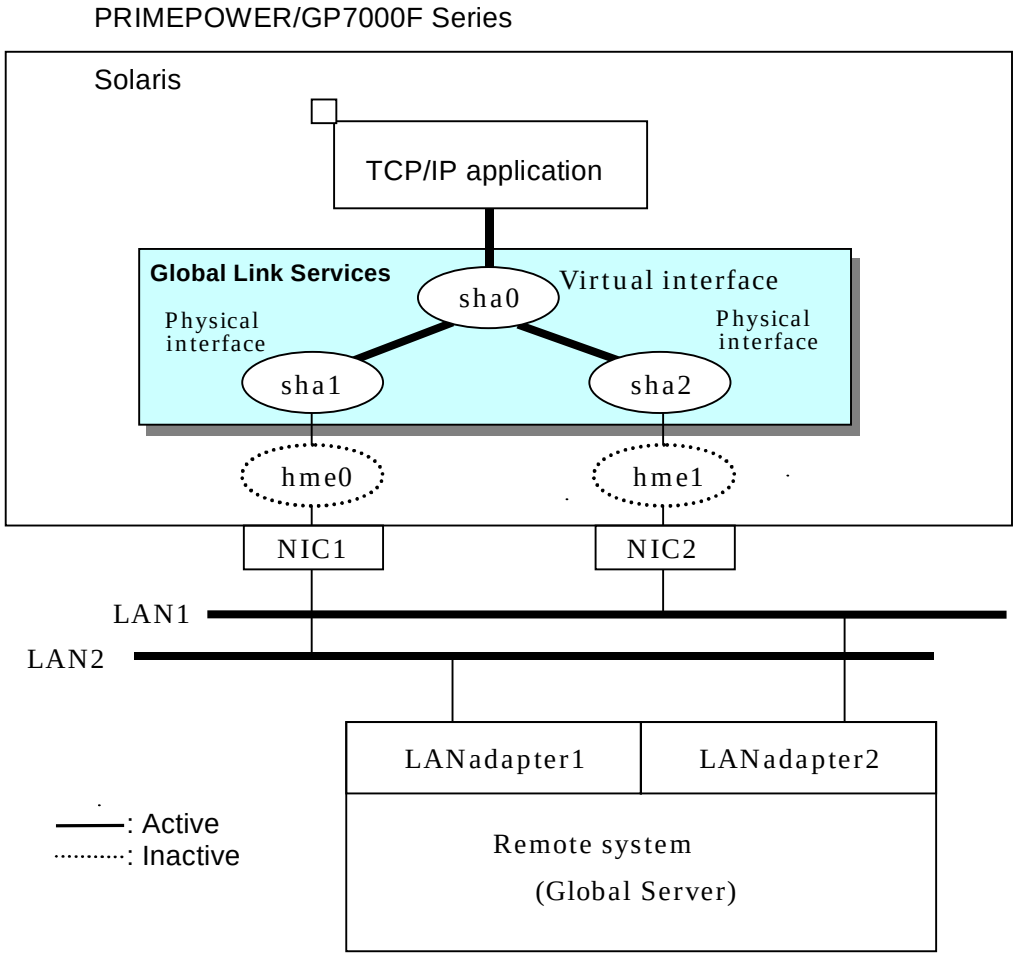


Figure 1.9 GS/SURE linkage mode (GS/SURE connection function)

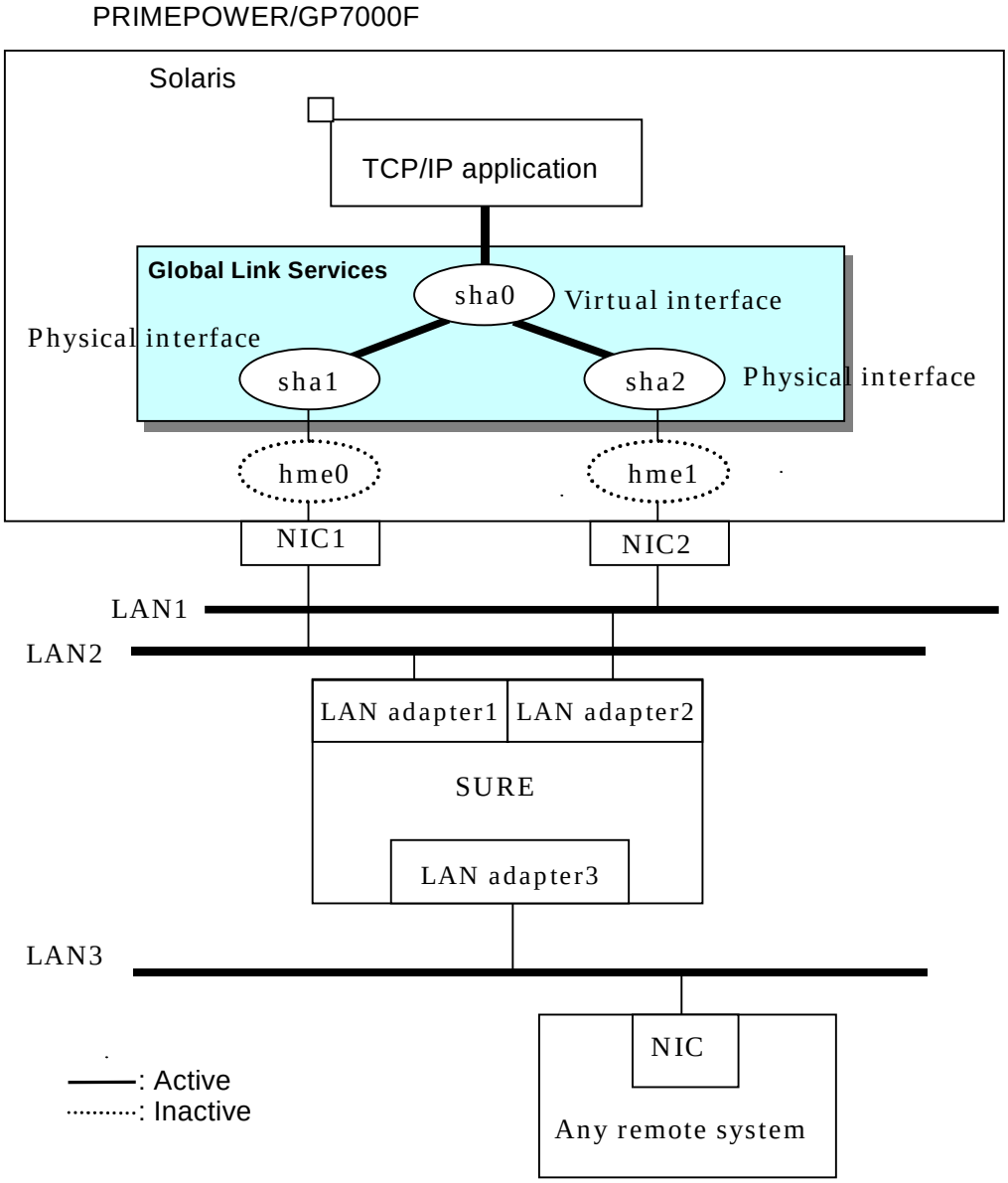


Figure 1.10 GS/SURE linkage mode (TCP relay function)

Redundant Line Control function consists of the following components:

Network device		PRIMEPOWER, GP7000F Series
NIC (Network Interface Cards)		The following Fujitsu adapters or cards can be used: - Basic Ethernet interface - Ethernet adapter or card - Fast Ethernet adapter or card - Quad Fast Ethernet adapter or card - Gigabit Ethernet adapter or card - InfiniBand (*1) host channel adapter or card (Available for fast switching mode only) *1: InfiniBand is a trademark and/or service mark of the InfiniBand Trade Association.
Router (RIP mode)		The following router is recommended: - Fujitsu LINKRELAY Series
HUB (NIC switching mode)		IP address information must be configured for HUB, e.g. HUB with SNMP agent
Operating system (OS)		- Solaris 8 (32-bit and 64-bit modes) - Solaris 9 (32-bit and 64-bit modes) - Solaris 10
Interfaces	Physical interface	Generated by each NIC. The interface name is determined by the NIC type (e.g. hmeX and qfeX). In GS/SURE linkage mode, physical interfaces are generated through redundant line control. The interface name is shaX.
	Tagged VLAN interface	Logical interface generated by NIC that supports a tagged VLAN (IEEE802.1Q). The interface name varies depending on NIC type (e.g. ce1000, fjgi2001)
	Virtual interface	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, the virtual interface name is used technically although no virtual interface is generated. A logical IP is allocated to the actual network so that the network applications enable communication through the logical IP address.
Network number	Fast switching mode, RIP mode, and GS/SURE linkage mode	A different network number is assigned to each physical interface and a virtual interface. In Figure 1.7, three network numbers must be prepared for the three interfaces.
	NIC switching mode	Only one number is assigned to each network. No virtual interface is generated
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.

	RIP mode, and GS/SURE linkage mode	An IP address must be allocated to each physical interface and a virtual interface. If there are two or more virtual interfaces, an IP address will be allocated to each virtual interface. Only IPv4 can be used.

Chapter 2 Feature description

This chapter outlines the functions and features of GLS.

2.1 Overview of Functions

2.1.1 Fast switching mode

In this mode, each 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.

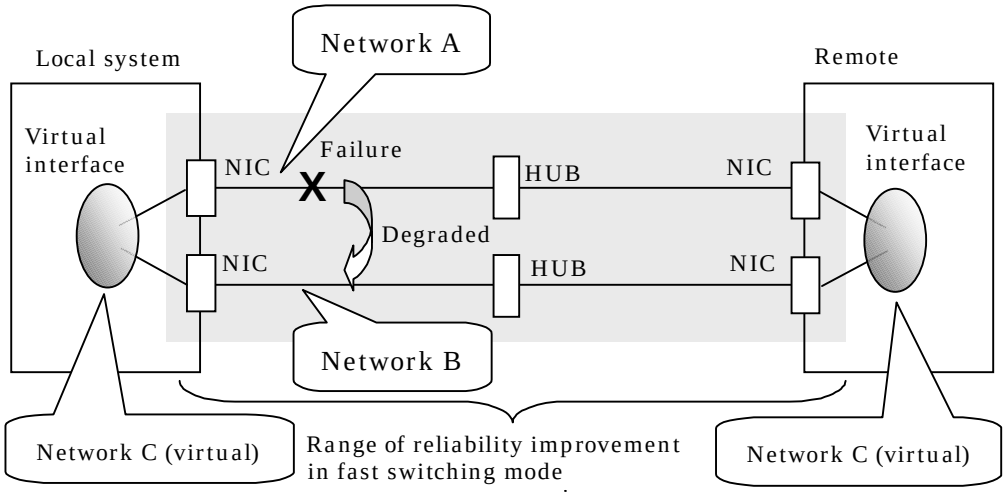


Figure 2.1 Example of duplicated operation in Fast switching mode

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.

Example of recommended application

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

System configuration

Figure 2.2 shows a system configuration for Fast switching mode:

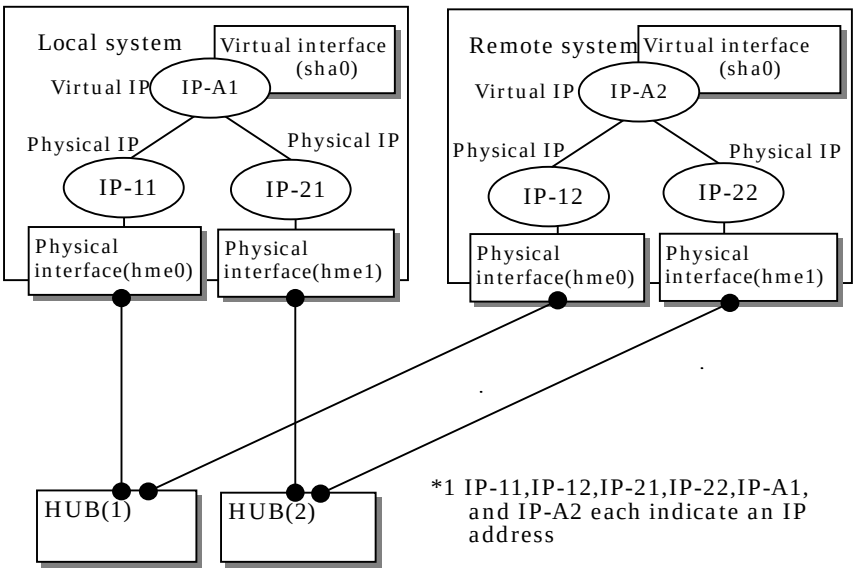


Figure 2.2 System configuration for Fast switching mode

The following explains each component and its meaning:

Physical interface

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

Physical IP

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

Virtual interface

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

Virtual IP

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

2.1.1.1 Fault monitoring function

Fault monitoring

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

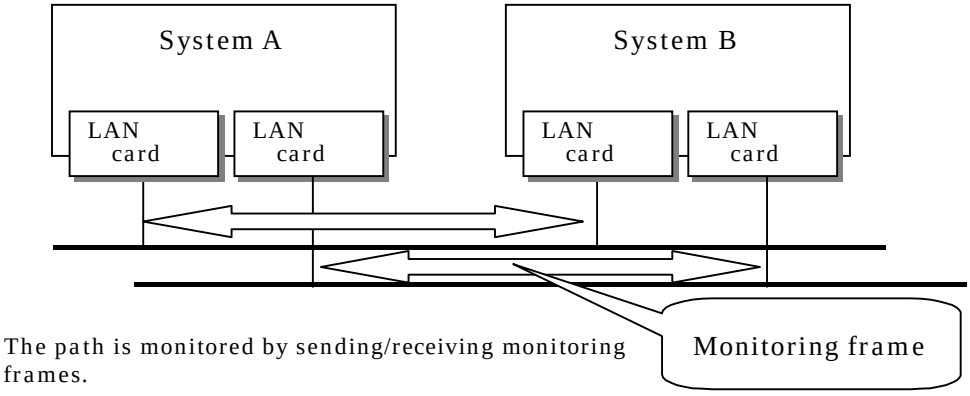


Figure 2.3 Monitoring method in Fast switching mode

Switching time

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

Detectable failures

The following failures can be detected:

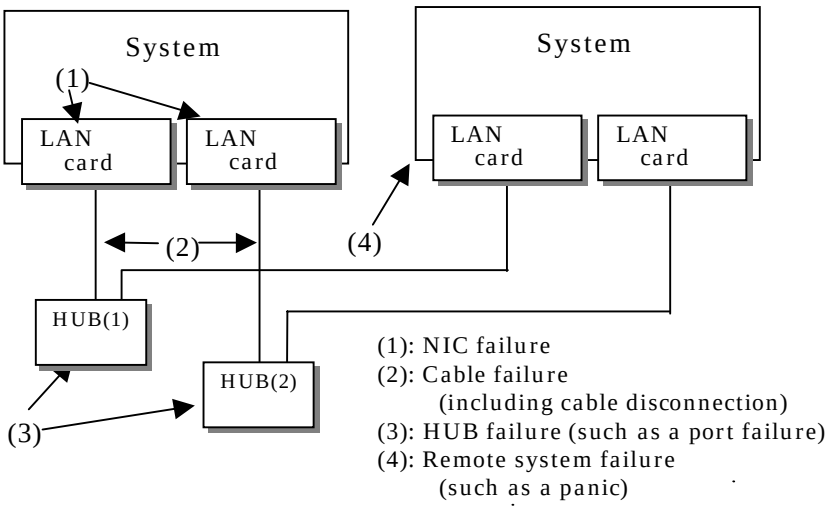


Figure 2.4 Detectable failures in Fast switching mode

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

Fault monitoring start/stop

Monitoring is started automatically when the virtual interface is activated. 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).

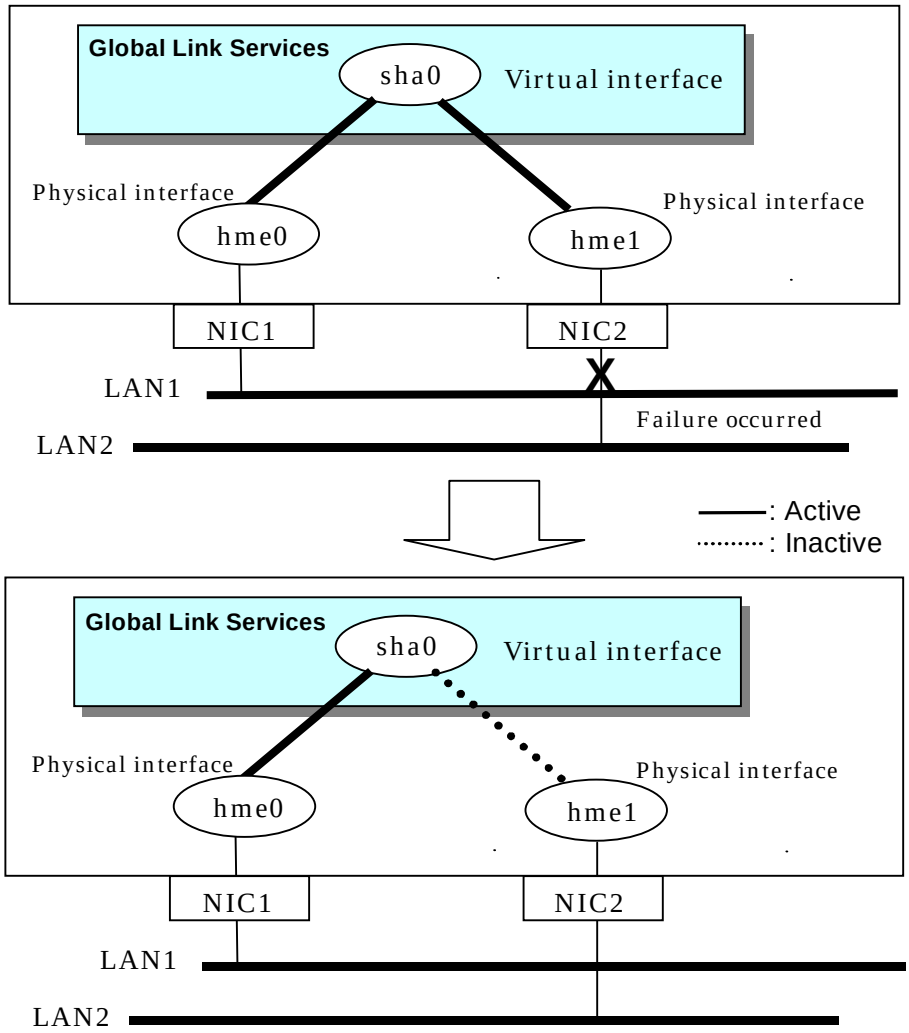


Figure 2.5 Outline of switching operation performed when a failure occurs in Fast switching mode

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:

- PRIMEPOWER
- GP7000F
- PRIMERGY
- PRIMEQUEST

2.1.1.4 Available application

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

- Application using the TCP or UDP.

2.1.1.5 Notes

- When assigning IPv4 address to the virtual interface, IPv4 address must be assigned to all the redundant physical interfaces.
- If assigning IPv6 address to the virtual interface, IPv6 address must be assigned to all the redundant physical interfaces.
- If assigning both IPv4 and IPv6 to the virtual interface, these two forms of an IP address must be assigned to all the redundant physical interfaces.
- No multi-cast IP address can be used.
- See "2.1.2.5 Notes" as to making into a subnet when using together with RIP mode.

2.1.2 RIP mode

In this mode, each of multiple NIC (Network Interface Card) is connected to a different network and all these NICs are activated.

Just as in Fast switching mode, a virtual interface is generated and a virtual network is allocated to this interface. 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 local system IP address.

The lines are monitored in accordance with the standard protocol on the Internet RIP (Routing Information Protocol). RIP is controlled by routing daemons (in.routed) on the Solaris system. The version of the routing daemons supported by the Solaris system is version 1.

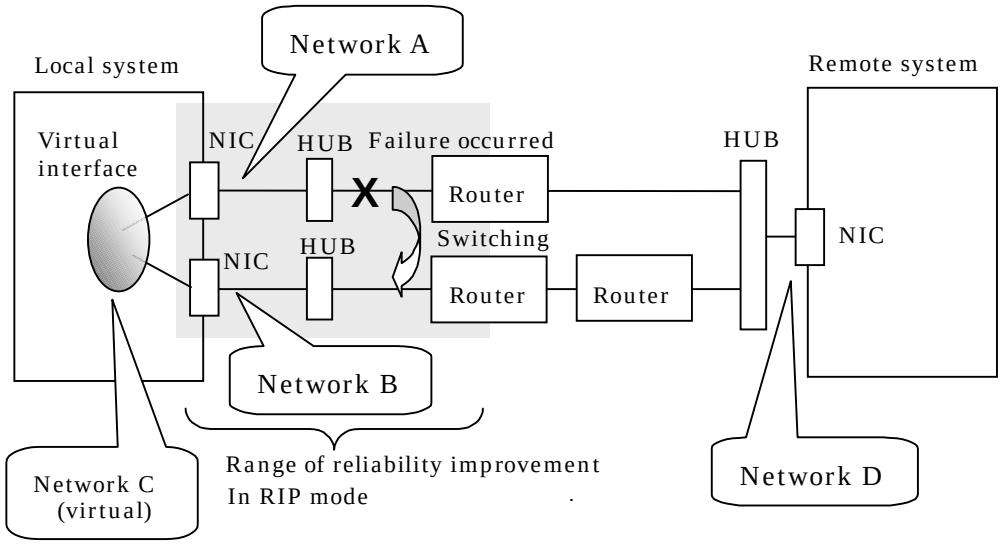


Figure 2.6 Example of duplicated operation in RIP mode

Connection type

Routers are placed between systems to enable communicate between them, with each communication route comprising a different network.

Features

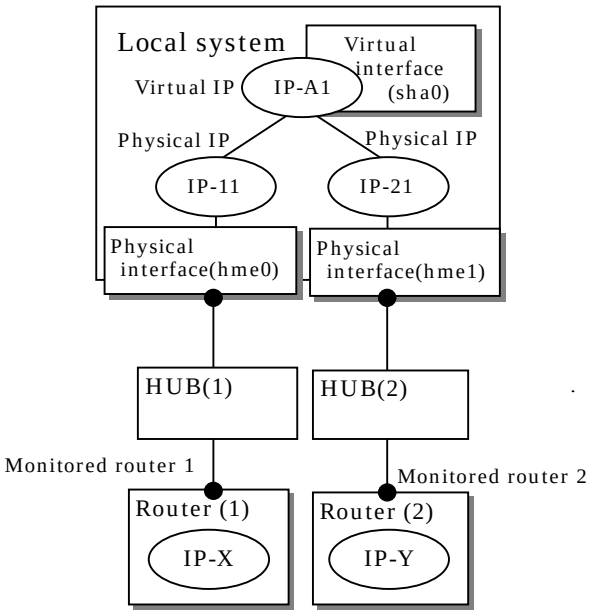
Because the Internet standard routing protocol RIP is used, communication can be carried out with a variety of devices in a global network environment regardless of the models. However, because the path switching by RIP is performed slowly, switching requires some time.

Recommended application areas

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

System configuration

Figure 2.7 shows a system configuration for RIP mode:



*1 IP-11, IP-12, IP-A1, IP-X, and IP-Y each indicate an IP address.

Figure 2.7 System configuration for RIP mode

The following explains each component and its meaning:

Physical interface

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

Physical IP

Indicates an IP address attached to a physical interface. This IP address is always active. IPv4 address can be used for a physical interface.

Virtual interface

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

Virtual IP

Indicates a local IP address to be allocated to the virtual interface for communication with remote devices. IPv4 address can be used for a physical interface.

Monitored router 1

Indicates the IP address of a router to be monitored first when the router monitoring function is used.

Monitored router 2

Indicates the IP address of a router to be monitored after switching.

2.1.2.1 Fault monitoring function

Fault monitoring

The shortest path to the remote system is selected based on the RIP packet received from the neighboring router and the selected path is used for communication. Then, monitoring is carried out to check whether any RIP packet is received from the router. If a RIP packet is normally received, the transmission line is considered to be normal. If no RIP packet is received within a specified period of time, the transmission line is considered to be faulty and the line to be used for communication is switched in accordance with the routing information received from another router. Monitoring is carried out for each router connected to NIC. Routing control via RIP is performed by the Solaris system.

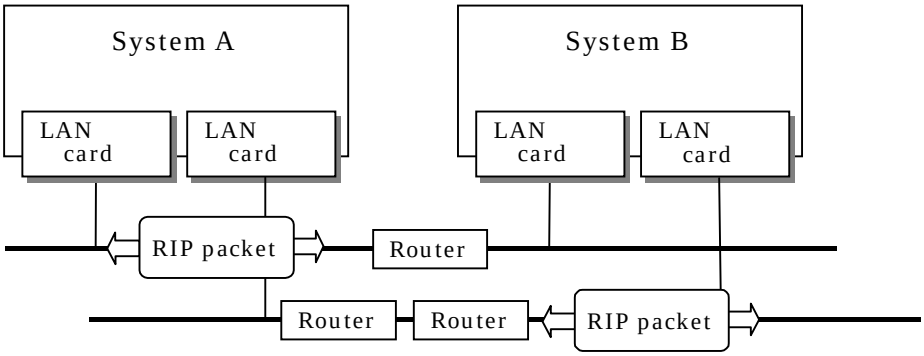


Figure 2.8 Monitoring method in RIP mode (when the router monitoring function is not used)

Switching time

If a failure occurs in a line, up to five minutes are required to switch the network paths via RIP.

Detectable failures

The following failures can be detected:

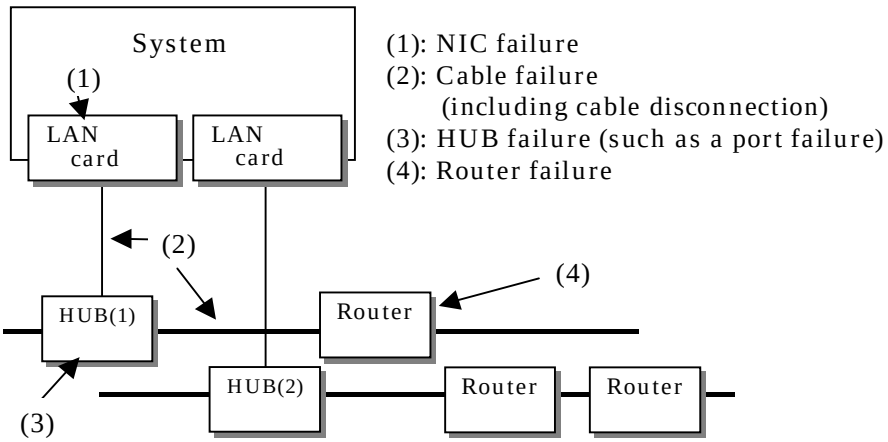


Figure 2.9 Effective monitoring range in RIP mode

Because the failures in (1) to (4) appear to be the same failure, it is not possible to determine under which of the four failure types these failures should be classified. Each device has to be checked to make this determination.

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, monitoring is started or stopped along with the start or stop of a RMS.

2.1.2.2 Switching function

Switching operation

The line is switched for use in communication in accordance with the routing information received from a router that is different from the router from which RIP was received.

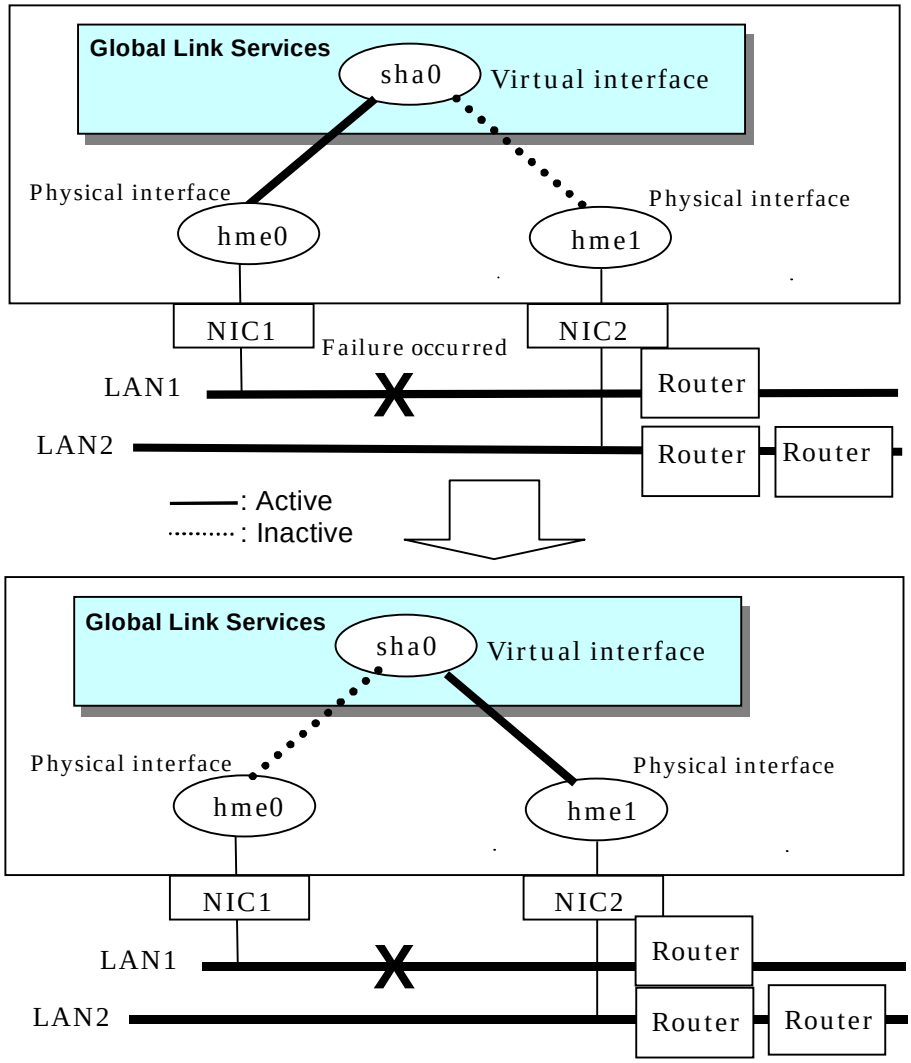


Figure 2.10 Outline of switching operation performed when a failure occurred in RIP mode

Failback operation

If a faulty line is recovered, the path is automatically restored to its original status in accordance with the RIP information. The failback of line cannot be performed manually.

2.1.2.3 Connectable remote host

Any system can be connected. However, the Fujitsu LINKRELAY Series is recommended as the router to be connected to the local system network.

2.1.2.4 Available application

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

- 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 (Applications of the remote party do not check the IP address).

2.1.2.5 Notes

- IPv4 address must be assigned to the physical interface.
- Only one machine should run on one network in RIP mode. If RIP is sent from more than one server, the propagation of path information becomes complicated and more time is required for switching than expected.
- No subnet can be created for a network to be used. Be sure to directly use a network of class A, B, or C without specifying a subnet mask. However, a subnet mask can be specified if the following conditions are met:

1. A subnet is created only for one network address.
2. A unique value in the entire network must be specified for the subnet mask for the network address for which a subnet is created.
3. A subnet mask value of the network address is defined in the /etc/netmasks file.

- It is not possible to use an IPv6 address.
- If you are using Solaris10 for OS, use the "routeadm(1M)" command to set up a routing daemon. See "3.2.2.3 System setup in RIP mode".

2.1.3 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.

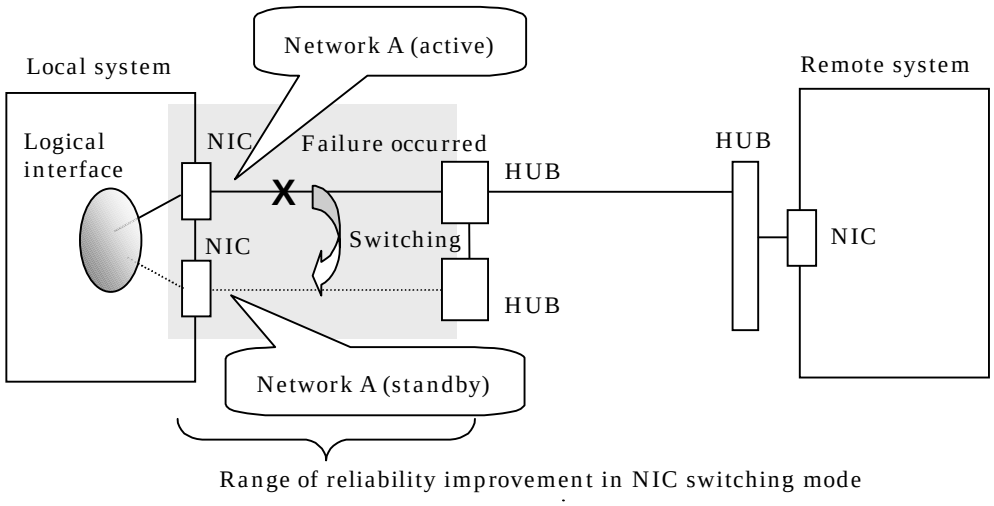


Figure 2.11 Example of duplicated operation in NIC switching mode

Information

NIC switching mode handles logical interface as a takeover interface. When using physical interfaces hme0 and hme1, the takeover interface becomes hme0:1 and hme1:1. Note that it is possible to takeover physical interface without using logical interface. Look under section "2.1.3.2 Switching function" for details on NIC switching mode.

Connection type

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

Features

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

Recommended application areas

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

System configuration

Figure 2.12 shows a system configuration for NIC switching mode:

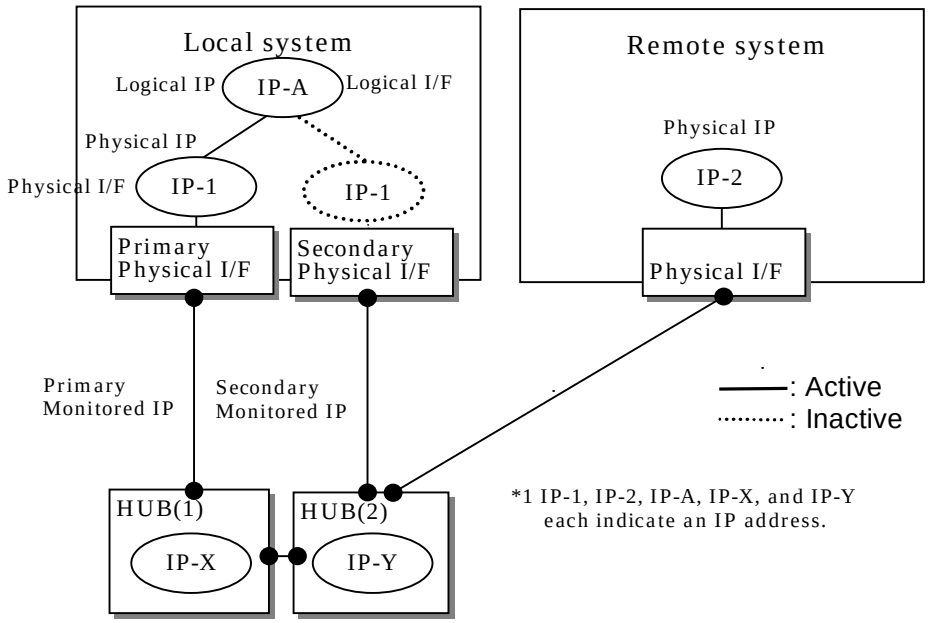


Figure 2.12 System configuration in NIC switching mode

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 addresss 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 "2.1.3.2 Switching function" about an physical IP address takeover function.

2.1.3.1 Fault monitoring function

Fault monitoring

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

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

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

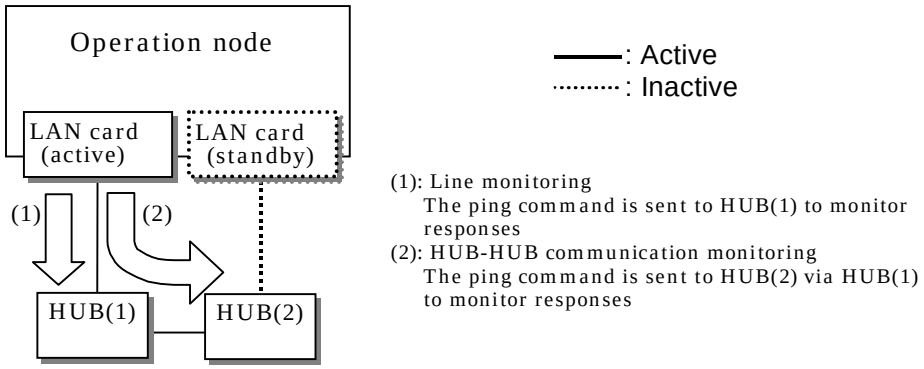


Figure 2.13 Monitoring method in NIC switching mode

Switching time

The switching time of a line is represented by [monitoring interval (sec) X monitoring count (count)] (for HUB-to-HUB communication monitoring, this is represented by [monitoring interval (sec) X monitoring count (count) X 2]). The monitoring interval can be set in the range of 1 to 300 seconds and the monitoring count can be set in the range of 1 to 300 times. By default, they are 5 seconds and 5 times respectively.

Even if the ping command failed immediately after started monitoring, it does not regard as a communication line failure until the waiting time (sec) for the Ethernet linkup passed. It is possible to set the waiting time for linkup in a range of 1 to 300 seconds and a default value is 60 seconds. However, if a value is smaller than [monitoring interval (sec) X monitoring count (count)], the time set for linkup is ignored and the time set by this [monitoring interval (sec) X monitoring count (count)] is adopted.

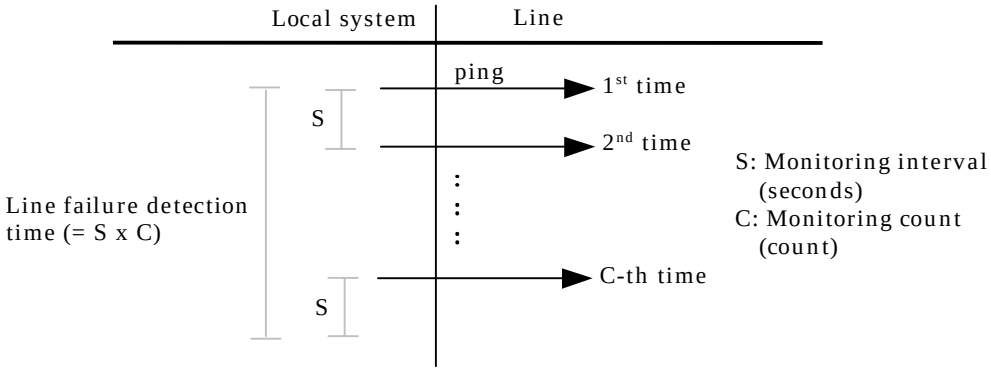


Figure 2.14 Fault detection time in NIC switching mode

Detectable failures

The following failures can be detected:

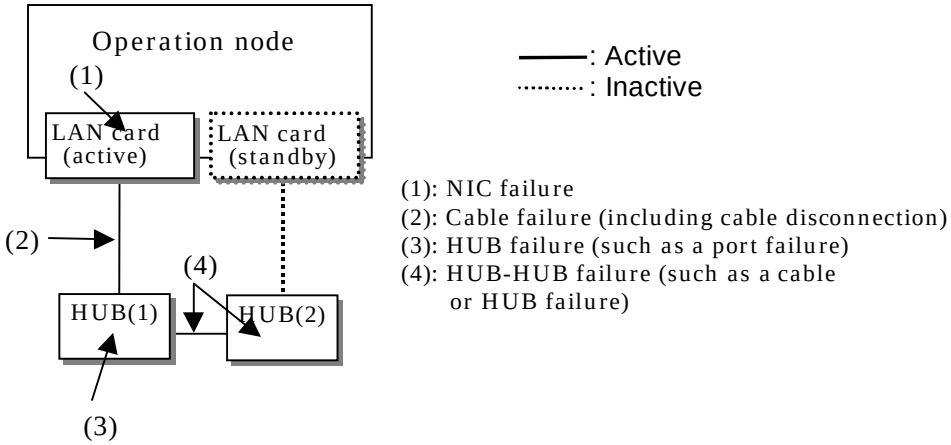


Figure 2.15 Effective monitoring range in NIC switching mode

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

Monitoring start/stop timing

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

2.1.3.2 Switching function

Switching operation

Switching operation changes the status of an active NIC into “down” and “unplumb” state and then changes the status of standby NIC to “plumb” and “up” so that standby NIC can run as a new active device. At this point, the MAC address and IP addresses (physical IP and logical IP) are taken over and then an ARP request packet is broadcast, in which the MAC address/IP addresses of the local node are set as the source.
It is possible to choose either a logical IP address takeover function or a physical IP address takeover function as an IP takeover mode.
Both a logical IP address and a physical IP address are taking over at the time of logical IP address takeover function use. Only a physical IP address is taking over at the time of physical IP address takeover function use, without activating a logical IP address.
When using an IPv6 address, it is not possible to use a physical IP address takeover function.
Figure 2.16 shows an example of node internal switching.

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

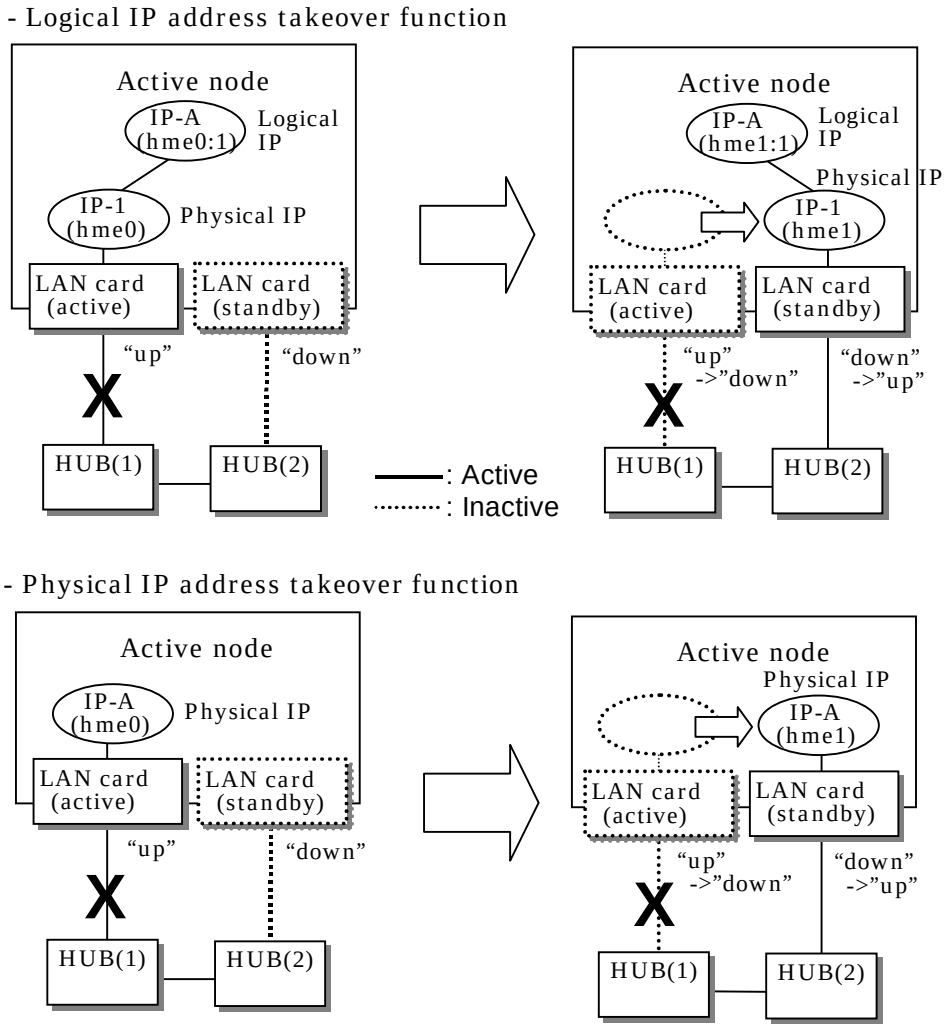


Figure 2.16 Outline of switching operation performed when a failure occurs in NIC switching mode

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.
Running this command makes recovered NIC to operate as an active NIC and recovers the system. In addition, if you setup a Standby Patrol Function, it automatically fails back the defective NIC without manually executing hanetnic change command. (For details regarding this operation, see "7.1 hanetconfig Command" and "7.9 hanetnic Command".) Furthermore, if in any case entire redundant NIC encounters failure, the monitoring process terminates. In such case, you must restart the process via hanetpoll off/on command after recovering the NIC. (For details on this command, see "7.7 hanetpoll 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.
- 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.)

2.1.3.5 Notes

- If assigning IPv4 address to the virtual interface, IPv4 address must be assigned to all the redundant physical interfaces.
- If assigning IPv6 address to the virtual interface, IPv6 address must be assigned to all the redundant physical interfaces.
- If assigning both IPv4 and IPv6 to the virtual interface, these two forms of an IP address must be assigned to all the redundant physical interfaces.
- No multi-cast IP address can be used.

2.1.4 GS/SURE linkage mode

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

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

As with Fast switching mode and RIP 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.

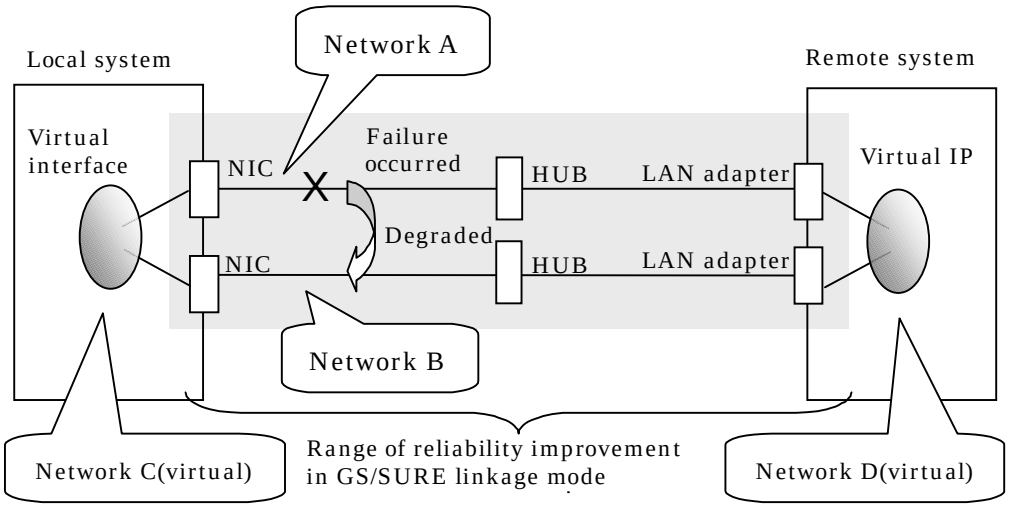


Figure 2.17 Example of duplicated operation in GS/SURE linkage mode

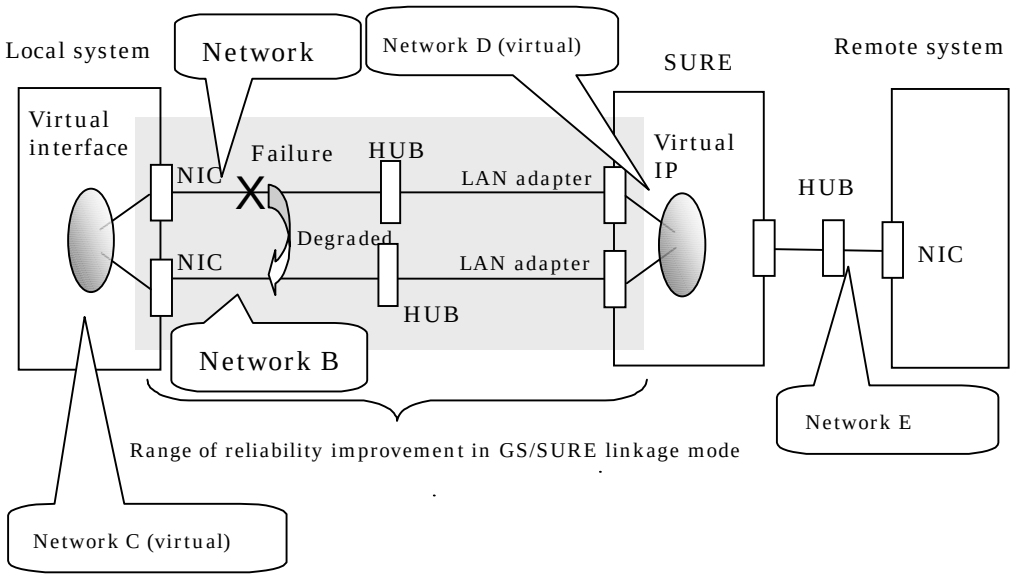


Figure 2.18 Example of duplicated operation in GS/SURE linkage mode (TCP relay function)

Connection type

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

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

Features

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

Examples of recommended application

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

System configuration

Figures 2.19 and 2.20 show a system configuration of GS/SURE linkage mode (GS/SURE communication function) and of GS/SURE linkage mode (TCP relay function), respectively.

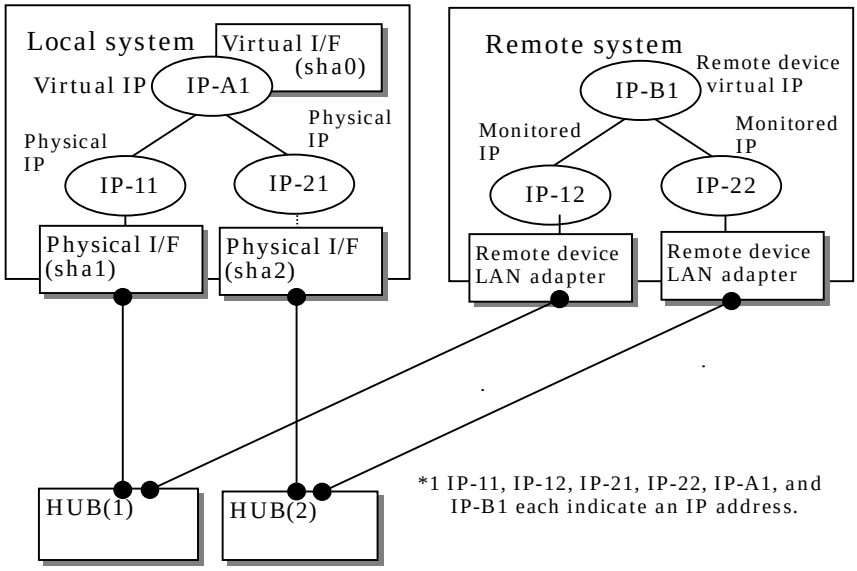


Figure 2.19 System configuration in GS/SURE linkage mode

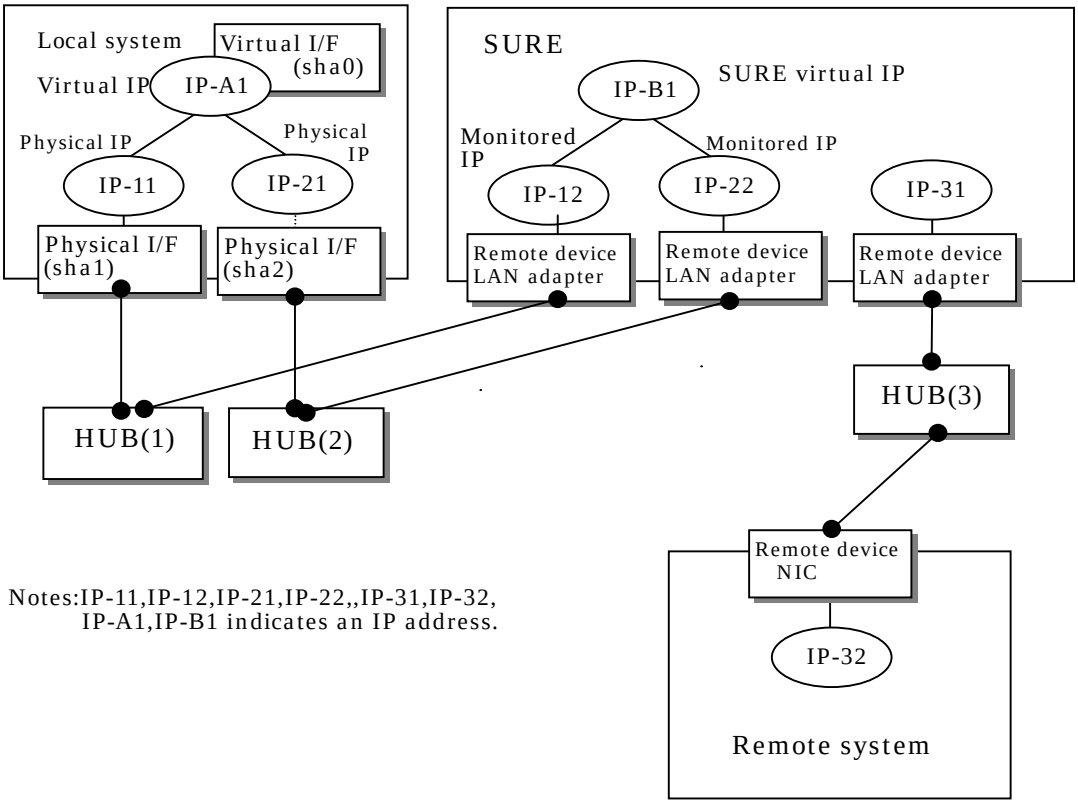


Figure 2.20 System configuration in GS/SURE linkage mode (TCP relay function)

The following explains each component and its meaning:

Physical interface

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

Physical IP

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

Virtual interface

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

Virtual IP

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

Relay device LAN adapter and remote device NIC

Indicates a NIC of the relay and remote devices.

Monitored IP

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

Remote device virtual IP

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

2.1.4.1 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.

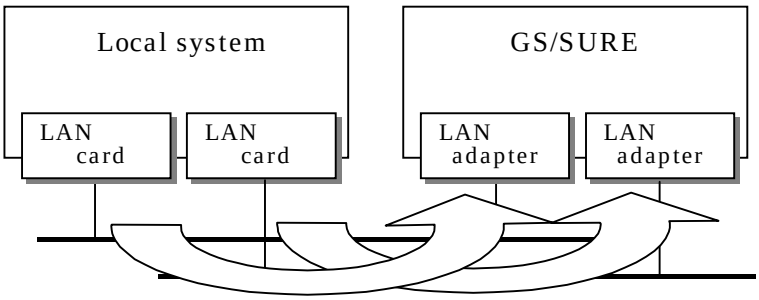


Figure 2.21 Monitoring method in GS/SURE linkage mode

Switching time

The switching 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:

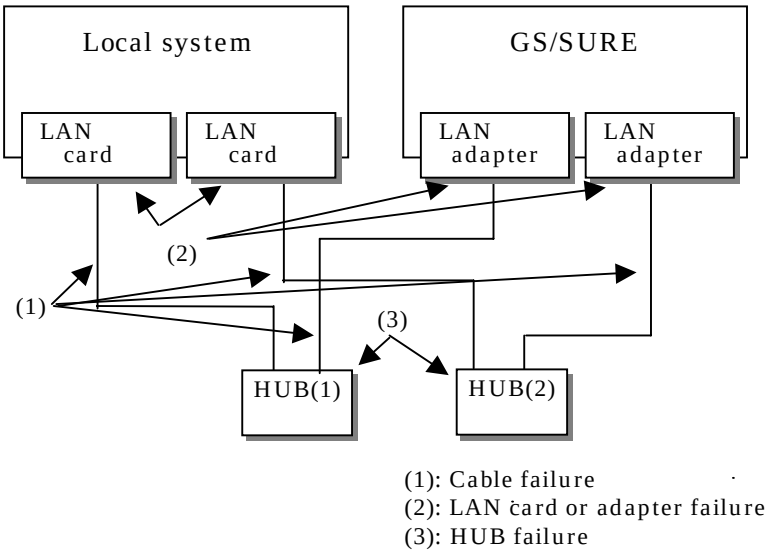


Figure 2.22 Detectable failures in GS/SURE linkage mode

Fault monitoring start/stop

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

2.1.4.2 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:

When using a GS/SURE communication function:

- GS (Global Server)
- SURE SYSTEM
- ExINCA

When using a TCP relay function:

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

2.1.4.4 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.

Thus, the Internet basic commands of Solaris such as ftp, telnet, and rlogin cannot be used in this mode.

2.1.4.5 Notes

- When using a physical interface, it is necessary to assign the IPv4 address.
- When using GS/SURE linkage mode (GS/SURE communication capability), the system must be configured as multi-homed host instead of a router.
  If you are using Solaris8 or Solaris9 for OS, create an empty file called /etc/notrouter then disable the router and IP forwarding. If you are using Solaris10 for OS, use the "routeadm(1M)" command. See "3.2.2.6 System setup in GS/SURE linkage mode".
- RIP, Fast switching and RIP modes are not allowed to coexist in a single node. Additionally, this mode cannot be applied for communication between Solaris servers.

2.2 Option Functions

Table 2.1 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	RIP mode	NIC switching mode	GS/SURE linkage mode
Multiple virtual interface definition	A	A	A	A
Cluster failover because of a line failure	A	X	A	A
Concurrent operation with other modes via one virtual interface	A	A	X	X
Sharing function of physical interface	A	A	A	X
Multiple logical virtual interface definition	A	A	O	X
Single physical interface definition	A	A	A	A
Router/HUB monitoring	X	A	A	X
Communication target monitoring	O	O	X	A
Standby patrol	O	O	A	O
Automatic failback	O	O	A	O
Dynamic adding/deleting/switching of interfaces used	A	A	A	A
User command execution	X	X	A	A

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

2.2.1 Configuring multiple virtual interfaces

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

Figure 2.23 below shows the concept of defining two virtual interfaces.

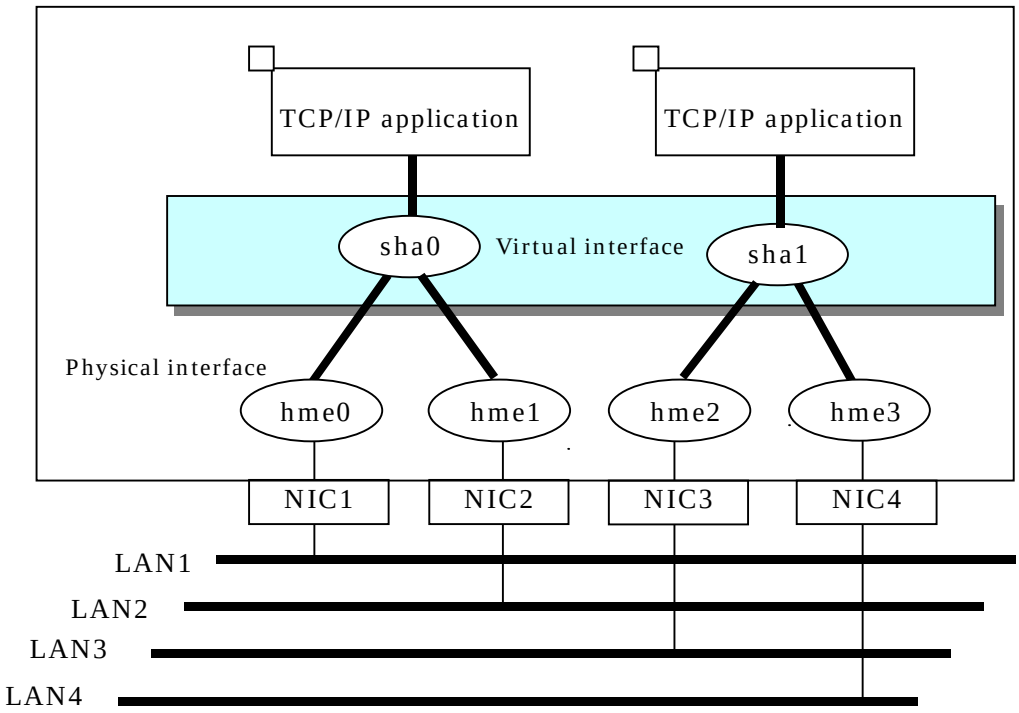


Figure 2.23 Two virtual interfaces being defined

2.2.2 Cluster fail-over when entire transfer routes fails

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

Figure 2.24 shows example of fail-over to node B when communication is disabled via both hme0 and hme1 bundled with virtual interface sha0 on node A.

Information

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

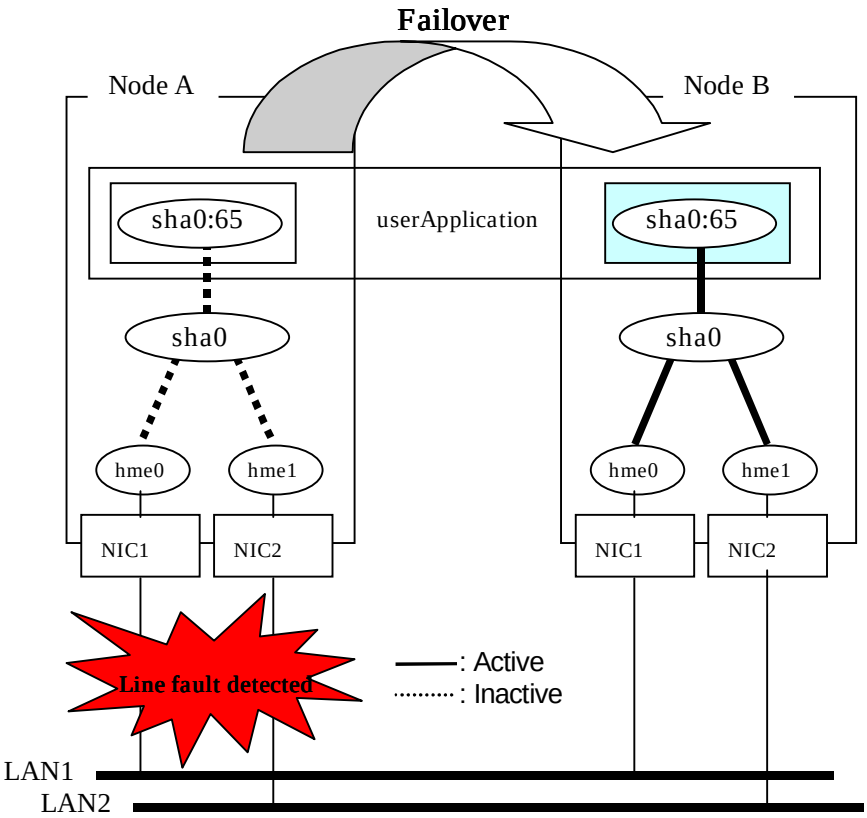


Figure 2.24 Cluster failover due to line fault

2.2.3 Operating several modes concurrently on a single virtual interface

You can operate both Fast switching mode and RIP mode concurrently via a single virtual interface. Fast switching mode is automatically selected for intra-network communications, and RIP mode for inter-network communications. A single virtual interface supports communications within the same network and between different networks.

Figure 2.25 shows the concept of Fast switching/RIP mode operation.

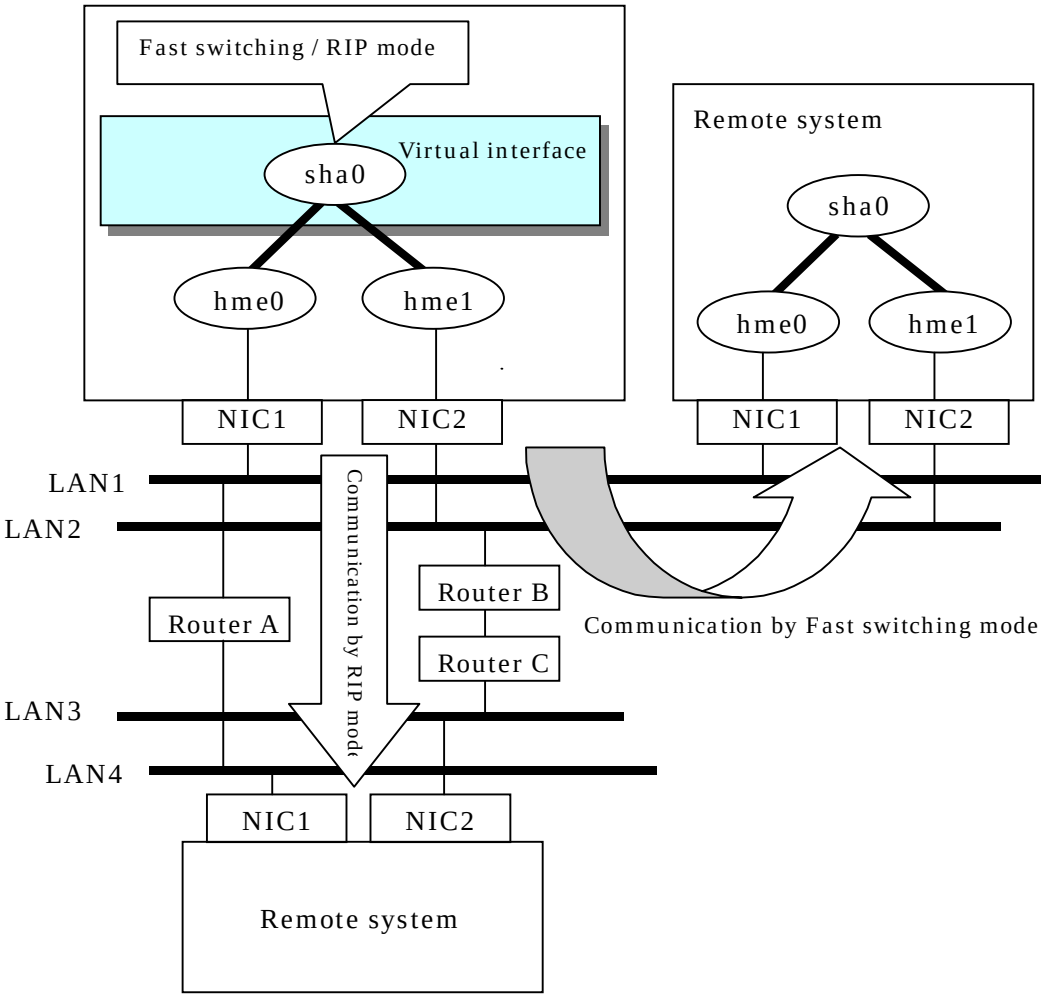


Figure 2.25 Fast switching mode / RIP mode operation

Note

- This function is only available for Fast switching and RIP mode. Other modes such as NIC switching mode and GS/SURE linkage mode cannot use this function.

2.2.4 Sharing physical interface

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

Using this capability, it is possible to:

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

2.2.4.1 Using Fast switching mode, RIP mode, and Fast switching/RIP mode

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

Figure 2.26 shows an example of three virtual interfaces, sha0 (Fast switching mode), sha1 (RIP mode), and sha2 (Fast switching/RIP mode) sharing three physical interfaces hme1, hme2, and hme3.

Note

Disparate network address can be assigned to a virtual interface of individual mode.

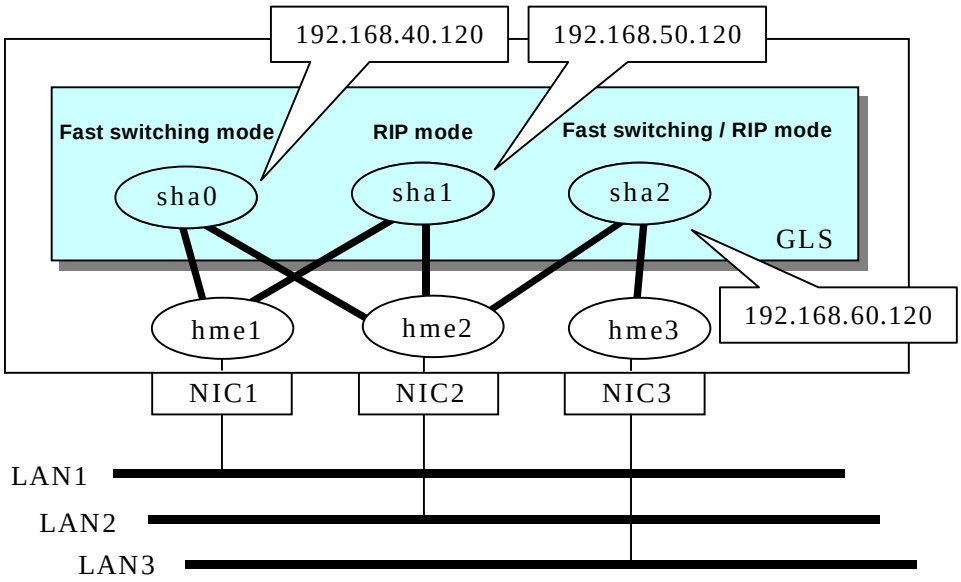


Figure 2.26 Example of sharing physical interface (1)

2.2.4.2 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, RIP mode, and GS/SURE linkage mode.

Figure 2.27 shows an example of three virtual interfaces sha0, sha1 and sha2 (all in NIC switching mode) sharing two physical interfaces hme1, and hme2.

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

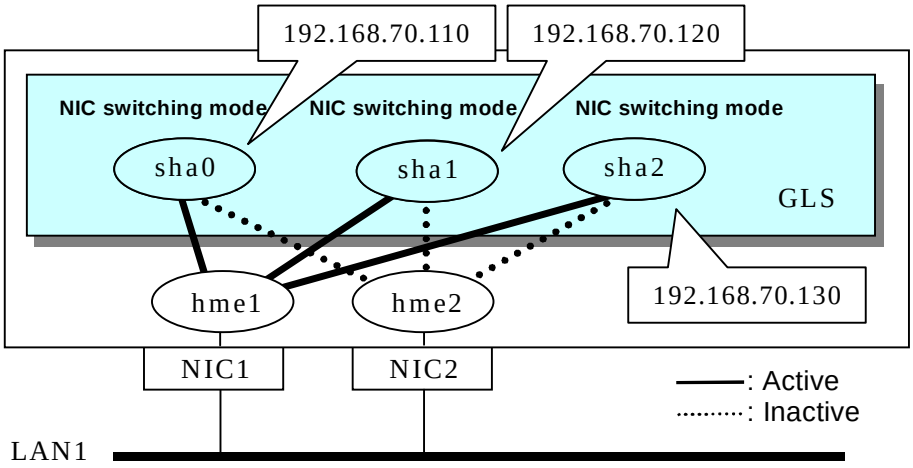


Figure 2.27 Example of sharing physical interface (2)

2.2.4.3 Using GS/SURE linkage mode

Cannot share physical interface.

2.2.4.4 Notices

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

2.2.5 Configuring multiple logical virtual interfaces

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

Figure 2.28 shows an example of defining three IP addresses (logical virtual interface) on a single virtual interface sha0.

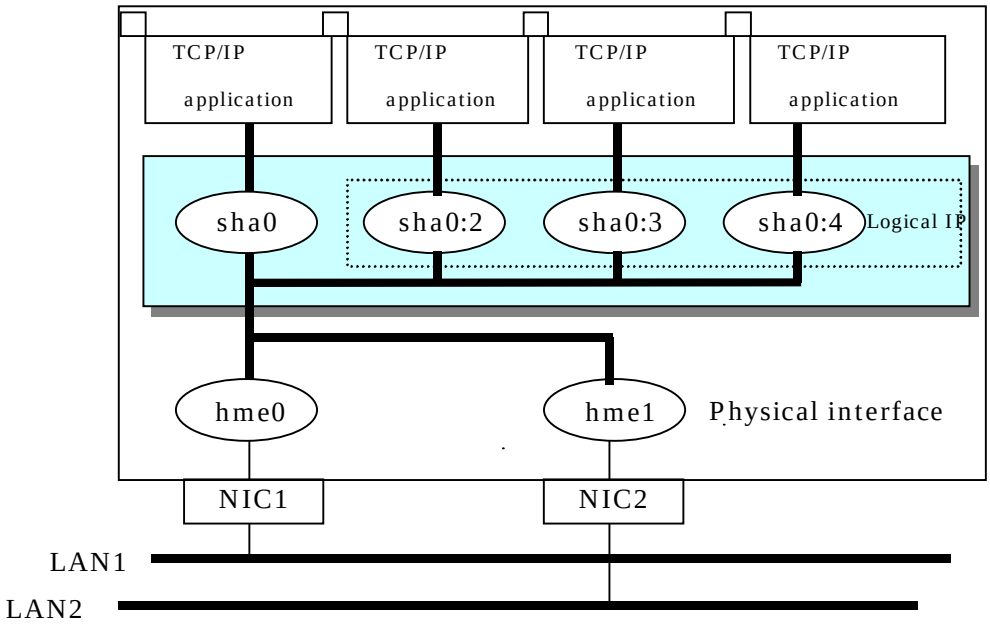


Figure 2.28 Logical virtual interfaces being defined

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

Note

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

2.2.6 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 shows an example of single physical interface configuration.

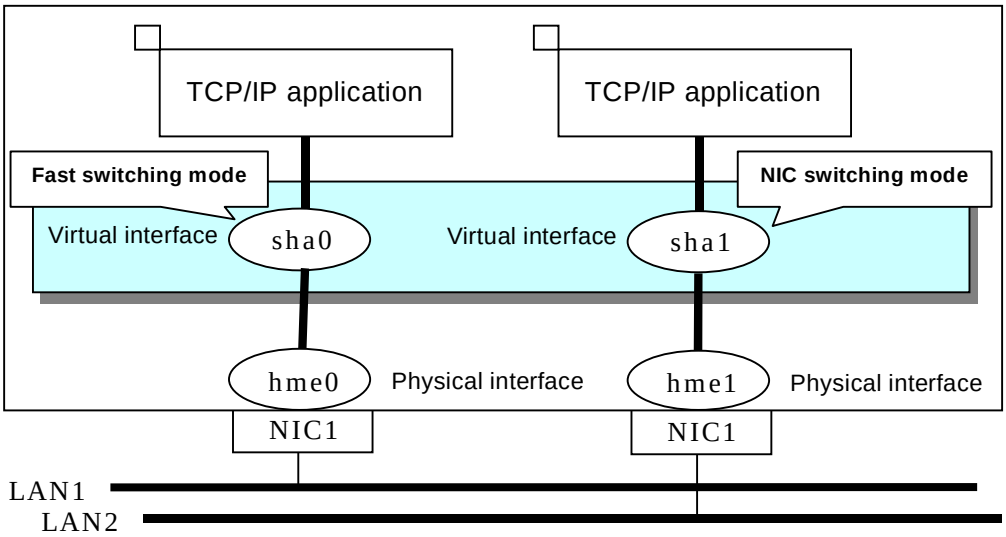


Figure 2.29 Single physical interface configuration

2.2.7 Router/HUB monitoring function

This section describes Router monitoring function for RIP mode as well as HUB monitoring function for NIC switching mode.

2.2.7.1 Router monitoring function

The router monitoring function switches transfer path by running the ping command to adjacent routers (up to two routers can be registered per virtual interface) at regular intervals and restarts in.routed if a line failure is detected. This function is available exclusively for RIP mode.

Without router monitoring function, when a failure occurs, switching transfer path takes approximately 5 minutes. However, using monitoring function switching transfer path only takes approximately 1 minute.

- If there is a different node running a routing daemon in the same network, the time taken to switch the transfer path may not be shortened.
- Depending on where the failure occurred, the time takes to switch the transfer path may not be shortened.
- With the Router monitoring function for RIP mode, both configuration of the monitoring target for each virtual interface and start/stop of the router monitoring are not supported.

Figure 2.30 shows a summary of router monitoring function

Begin operation with ping monitoring against the primary monitoring router (router A in the figure below). If a failure is detected against the primary monitoring router, it restarts the routing daemon, stop the monitoring process to the primary monitoring router, and start monitoring the secondary monitored router. For connection type, connection between other networks is possible.

To control the traffic, refer to the RIP information and use a single transfer path.

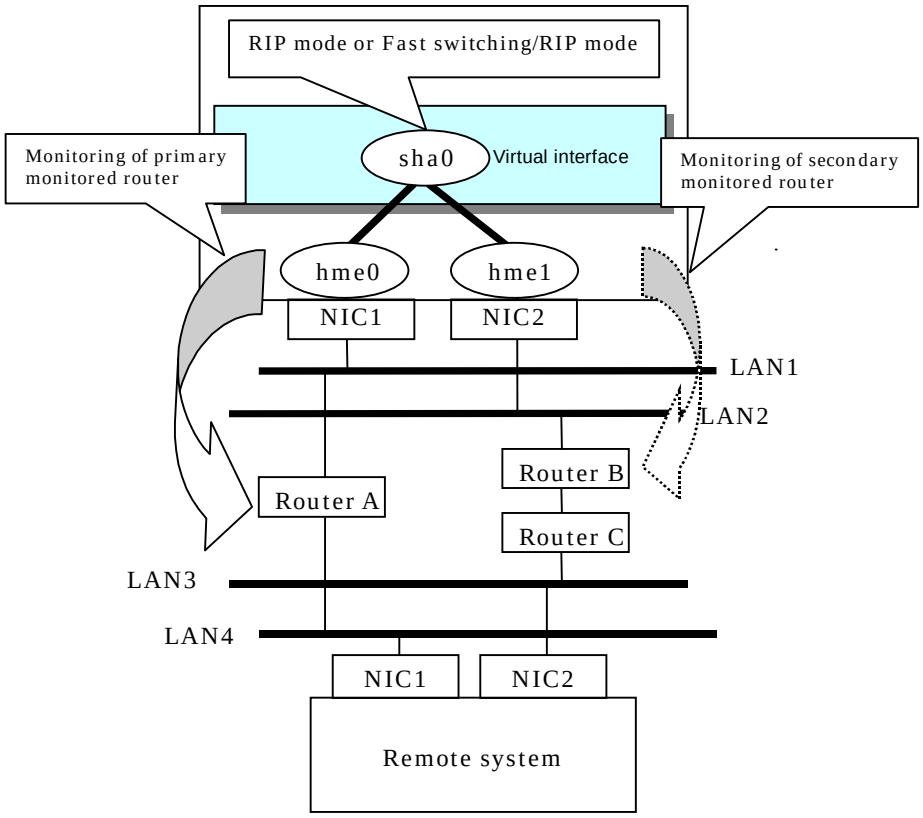


Figure 2.30 Router monitoring function

2.2.7.2 HUB monitoring function

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

Point

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

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

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 “2.2.9 Standby patrol function”)

Figure 2.31 shows an outline of the HUB monitoring function

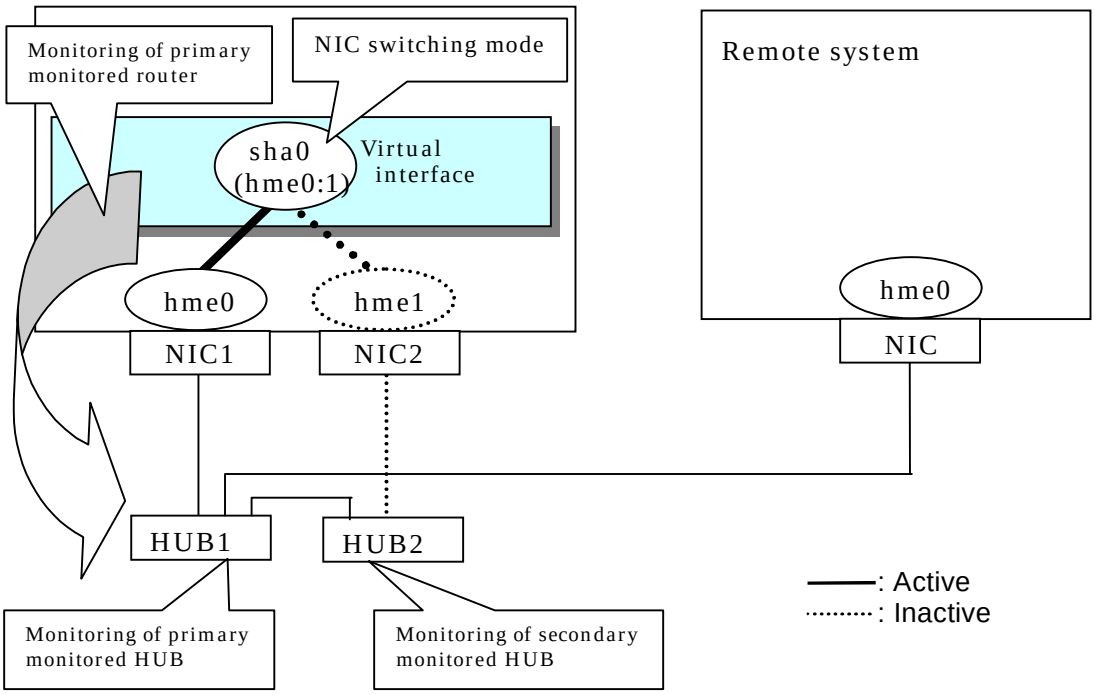


Figure 2.31 HUB monitoring function

Point

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

Note

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

2.2.7.2.1 Not using HUB-to-HUB monitoring feature

If the operation starts without HUB-to-HUB monitoring function, the primary HUB (HUB1 in the figure 2.32) is monitored using the ping command. When a failure is detected in the primary HUB, the NIC of the currently active system is inactivated and then the standby NIC is activated. After the standby NIC is activated, the secondary HUB (HUB2 in the figure 2.32) is monitored using the ping command.

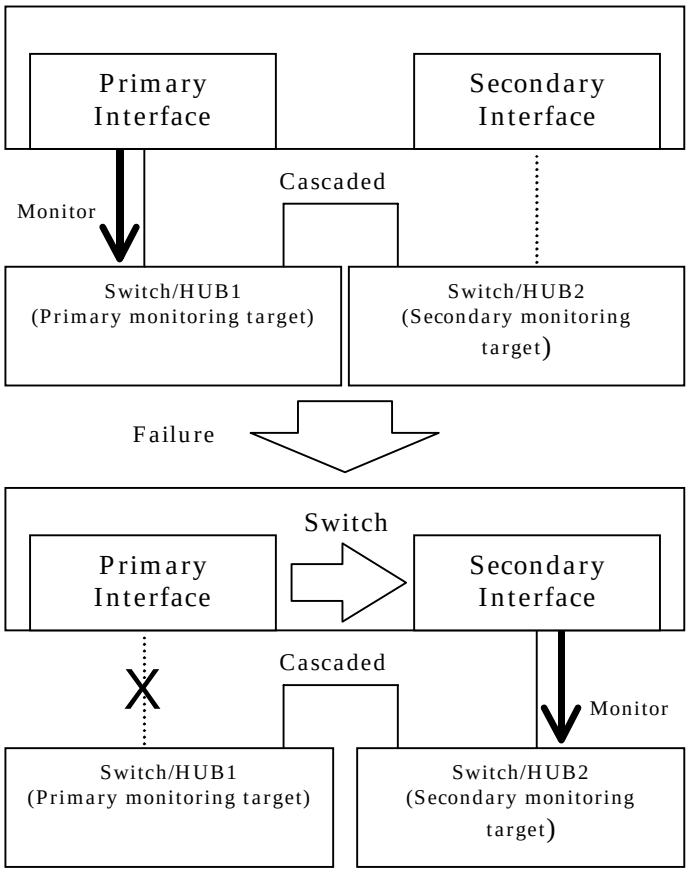


Figure 2.32 HUB-to-HUB monitoring disabled

2.2.7.2.2 Using HUB-to-HUB monitoring feature

If the operation starts using the HUB-to-HUB monitoring function, the secondary HUB (HUB2 in the figure 2.33) 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 (Swutch/HUB1 in Figure 2.33).
(During this occasion, a monitoring failure message (No.873) regarding the secondary HUB will be outputted. 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.873) 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.

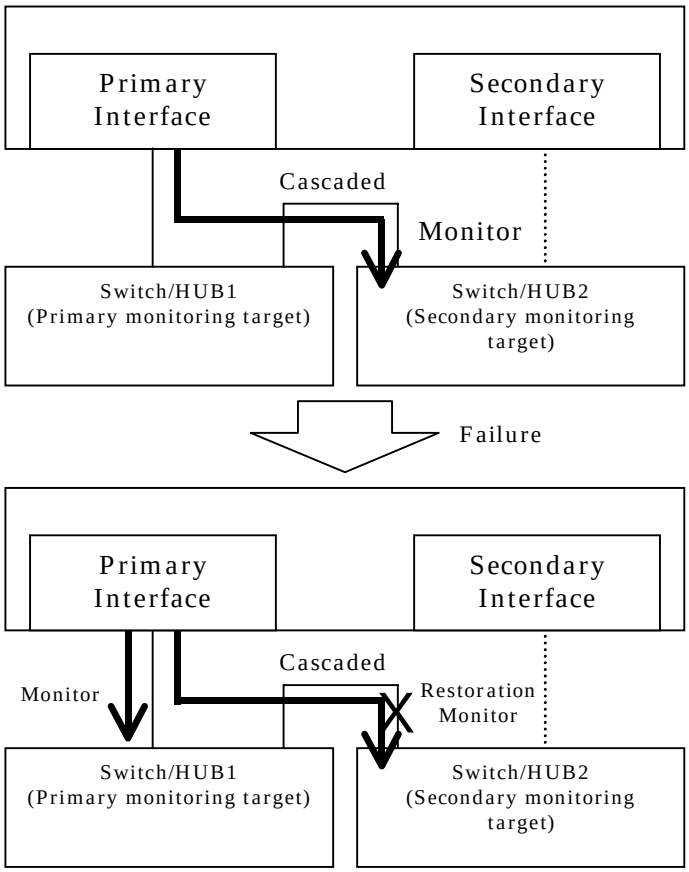


Figure 2.33 HUB-to-HUB monitoring enabled (failure on the secondary monitoring)

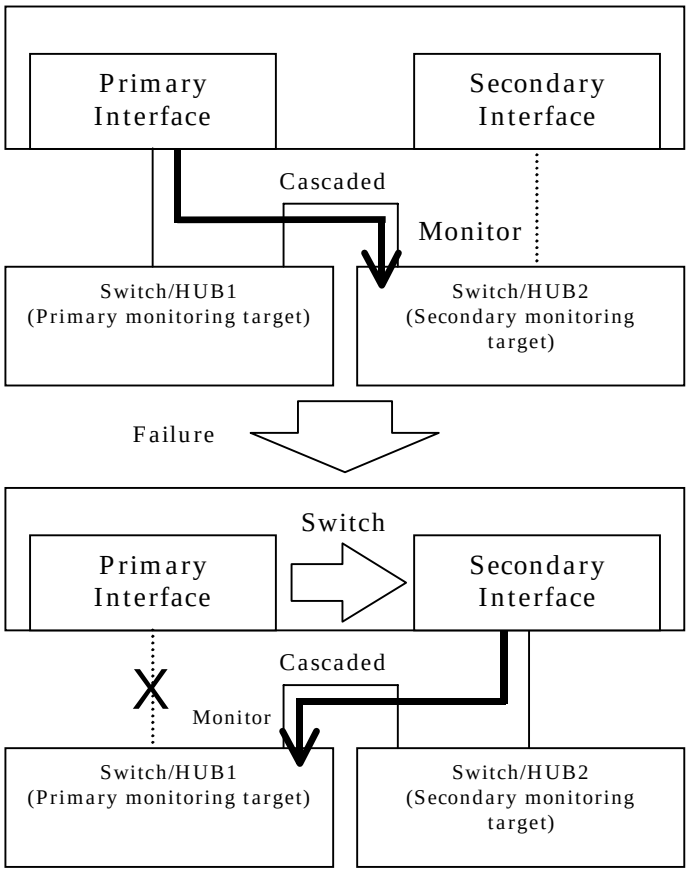


Figure 2.34 HUB-to-HUB monitoring enabled (failure on the primary monitoring)

2.2.7.2.3 Transfer path monitoring on individual virtual interface

On HUB monitoring function over NIC switching mode, it is possible to start/stop the transfer path monitoring for individual interface. It can also change the configuration parameters of monitoring frequency and monitoring interval for each virtual interface.

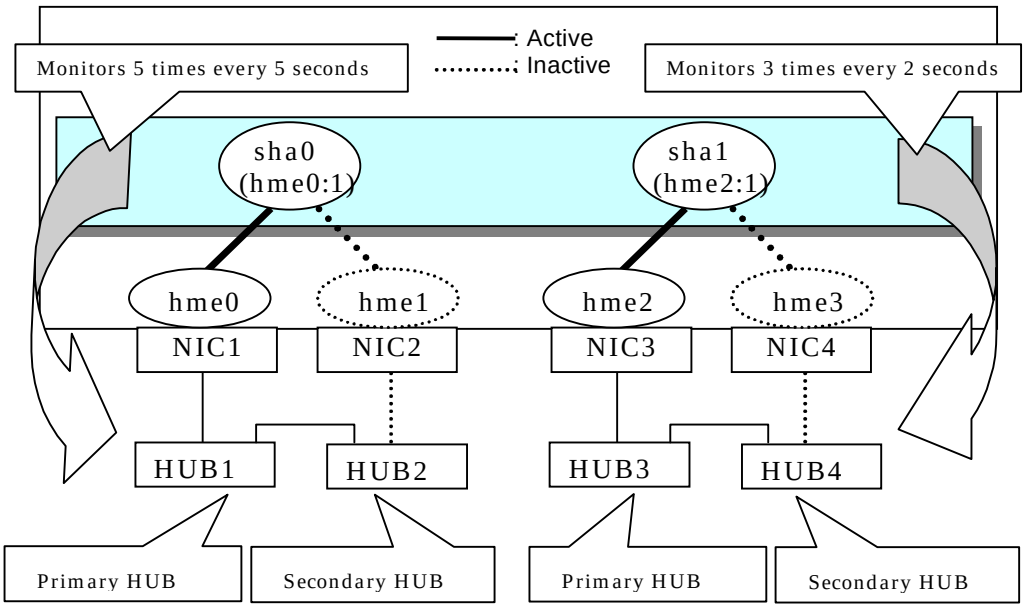


Figure 2.35 Monitoring on individual virtual interface

See

For details on configuring monitoring target for each virtual interface, refer to "7.7 hanetpoll Command".

2.2.8 Monitoring communicating host

In GS/SURE linkage mode, the ping command is issued against the IP address of the actual interface of the remote system at regular interval. If a transfer path failure is detected, a reporting message will be outputted. Then, communication is continued using other transfer path.

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

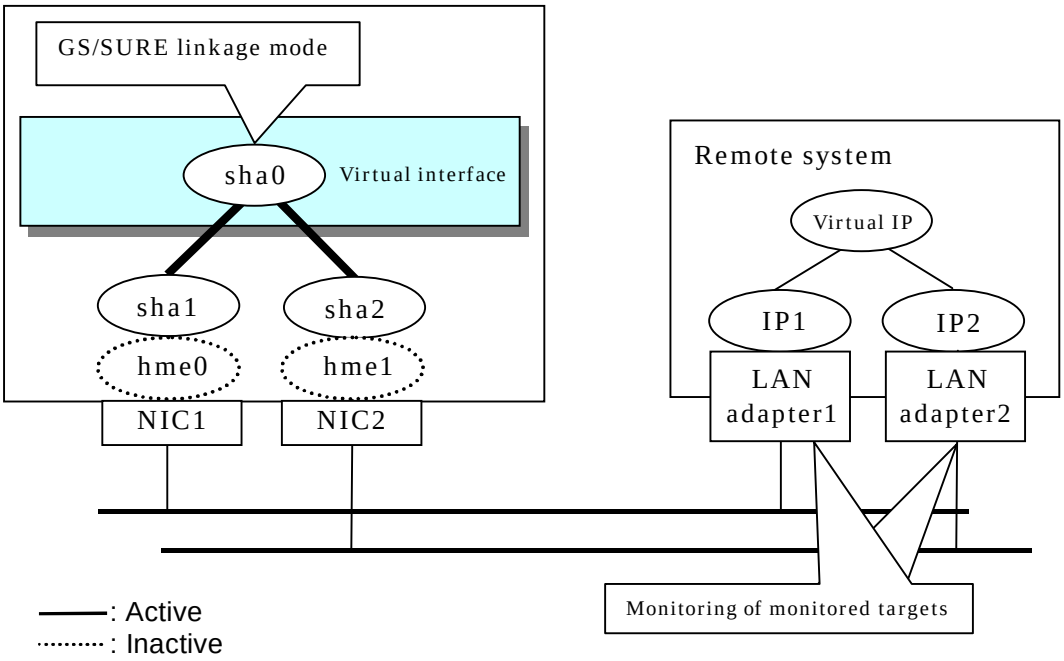


Figure 2.36 Remote system monitoring function

2.2.9 Standby patrol function

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

This brings the following effects:

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

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

See "2.2.10 Automatic fail-back" for an automatic fail-back function.

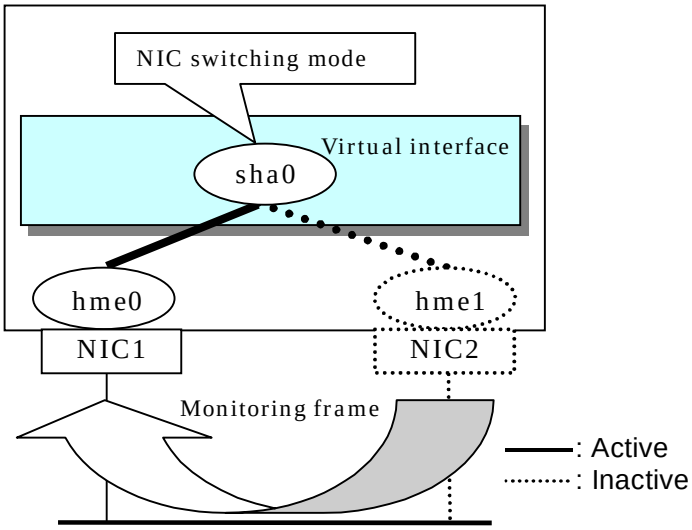


Figure 2.37 Standby patrol function

Note

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

2.2.10 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 2.38 shows the outline of the automatic fail-back function.

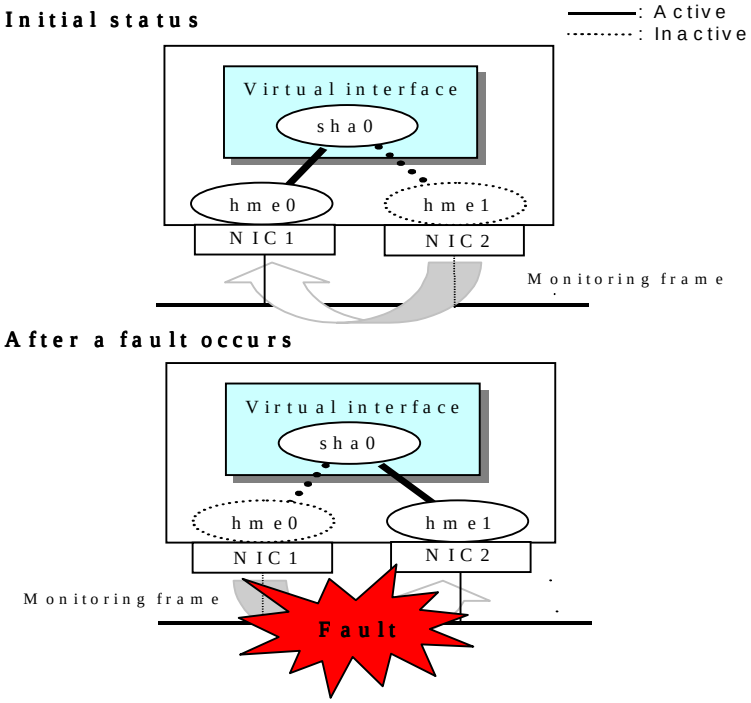


Figure 2.38 Automatic fail-back function (continued)

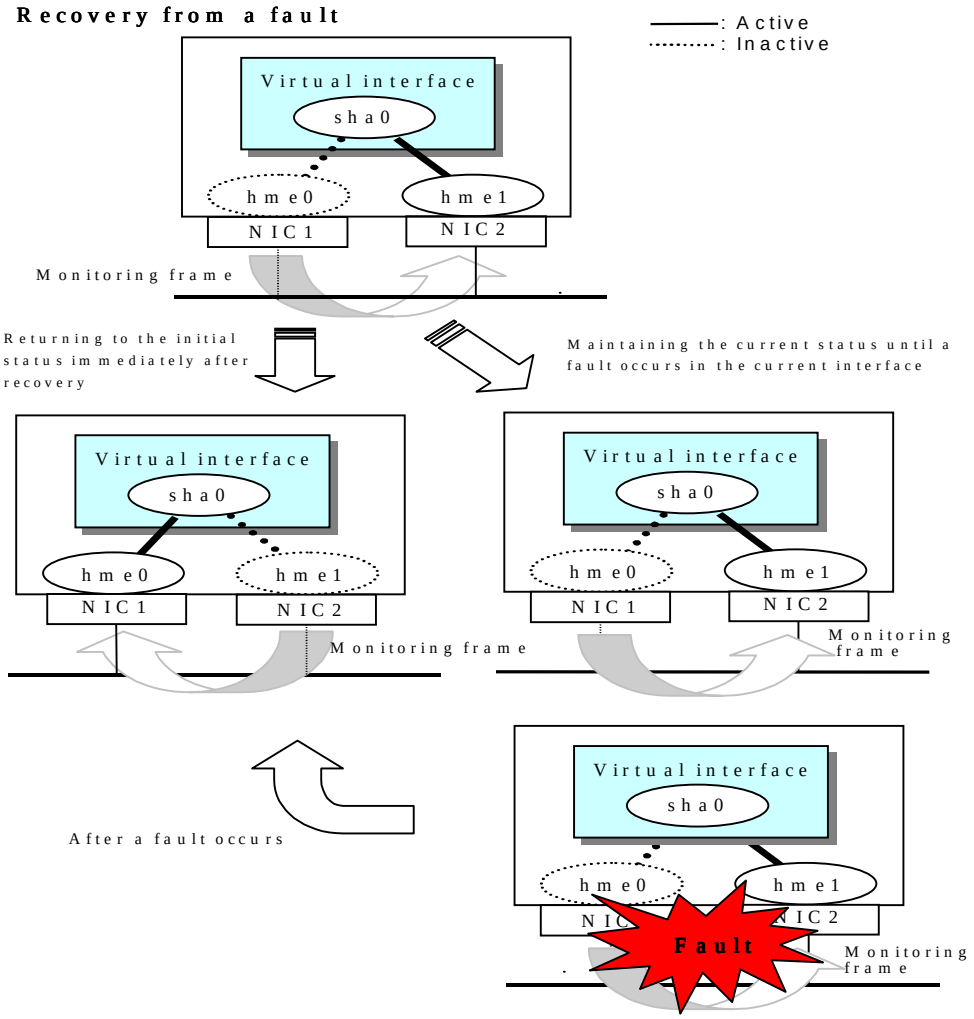


Figure 2.38 Automatic failback function (end)

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

Note

- After the failed interface is recovered, if a running interface fails before the Standby patrol detects the No.885 message indicating interface recovery, NIC switchback will not be executed. If this occurs, the Standby patrol will consider that both of the NICs are disabled until it detects the failed interface recovery. Recover the interface referring to "4.6.4 Recovery procedure from line failure in NIC switching mode".

2.2.11 Dynamically adding/deleting/switching physical interface

In Fast switching mode, RIP mode, Fast switching/RIP mode, and GS/SURE linkage mode (the operation mode is "c"), it is possible to add/delete bundled physical interfaces with a virtual interface kept activated (dynamic). The hanetnic command adds/deletes dynamically. See "7.9 hanetnic Command" for the detail.
Figure 2.39 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 is registered to the cluster resource.

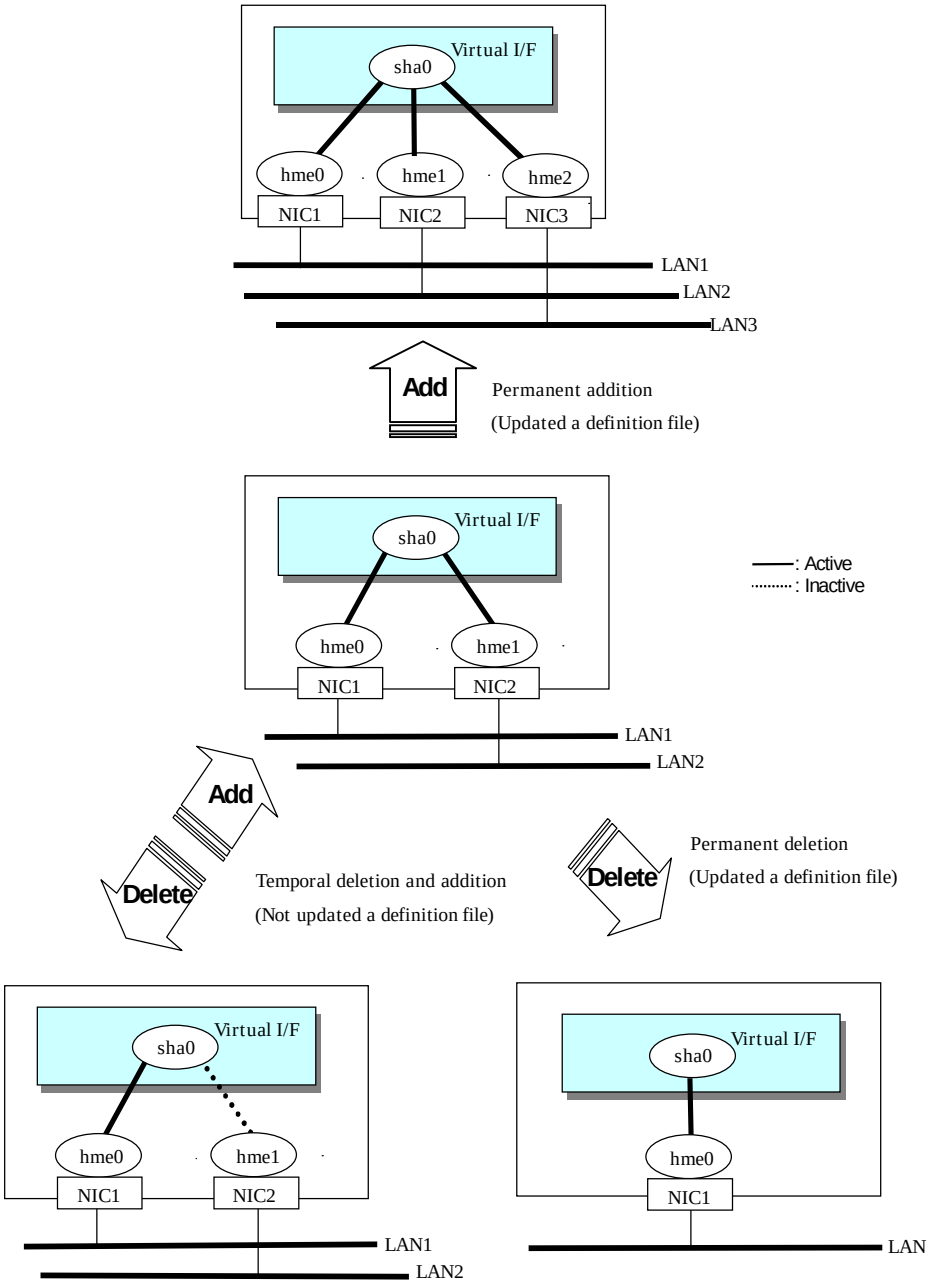


Figure 2.39 Dynamic adding/deleting function of physical interfaces used

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 2.40 shows an outline of operations performed when the physical interface switching command is executed. For information on the setup,

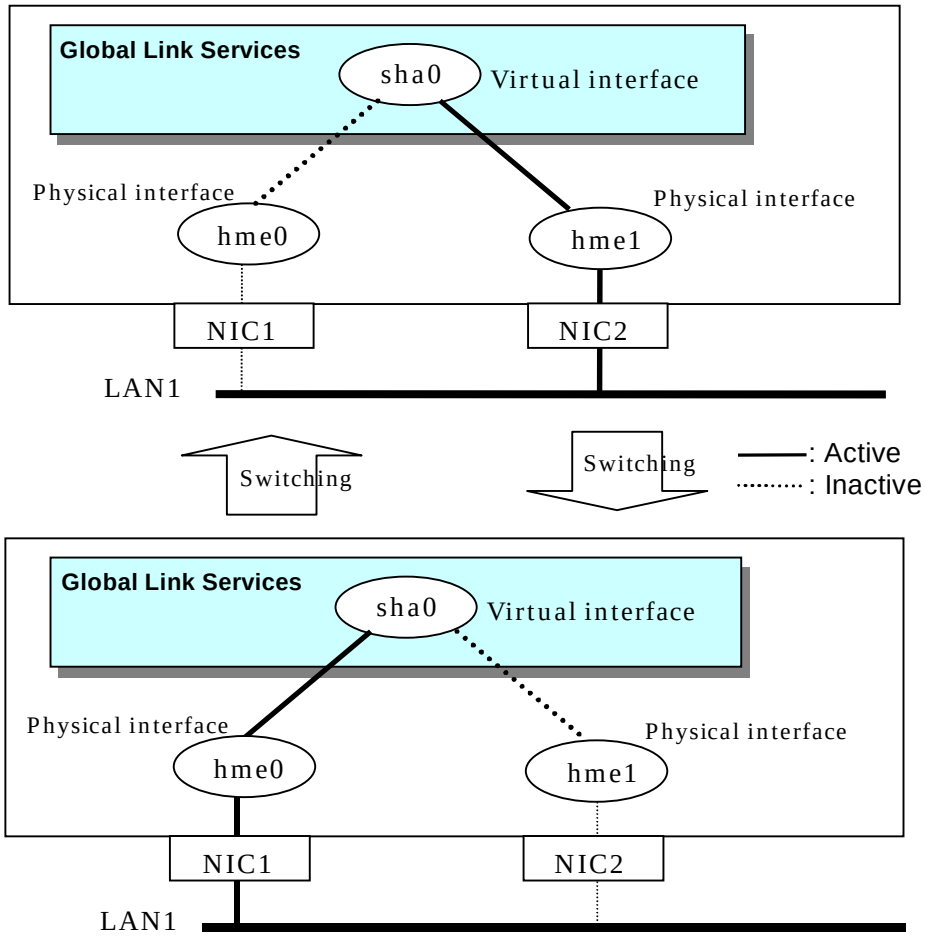


Figure 2.40 Dynamic switching function of physical interfaces used

2.2.12 User command execution function

In NIC switching mode and GS/SURE linkage mode, a user-defined command can be executed.

For information on the setup, see Section “3.6.11 Setting user command execution function".

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

Timing to run is as follows:

(1) NIC switching mode

- Running a user command when activated or deactivated an IP address
  Run a user specified command when activated or deactivated a logical IP address (when using a logical IP address takeover function) or a physical IP address (when using a physical IP address takeover function) by automatically switching due to an error in 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, to set the specified routing information, to delete the ARP information, and to change a MAC address.
- Running a user command when detected an error in a transfer route
  Run a user specified command when detected an error in monitoring a transfer route (such as LAN or HUB errors). Use this to notify a system administrator or an application of detecting an error.
- Running a user command when detected an error by standby patrol or recovery
  Run a user specified command when detected an error in monitoring a transfer route by standby patrol or recovery. Use this to notify a system adminitrator or an application of detecting an error or recovery. When set either of a monitoring interval ('-p' option) or the number of the times of continuous monitoring ('-o' option) of standby patrol to zero by a hanetparam command, it is not possible to use this user command execution function.

Figure 2.41 shows timing to run a user command when activated or deactivated an IP address in NIC switching mode (a logical IP address takeover function).

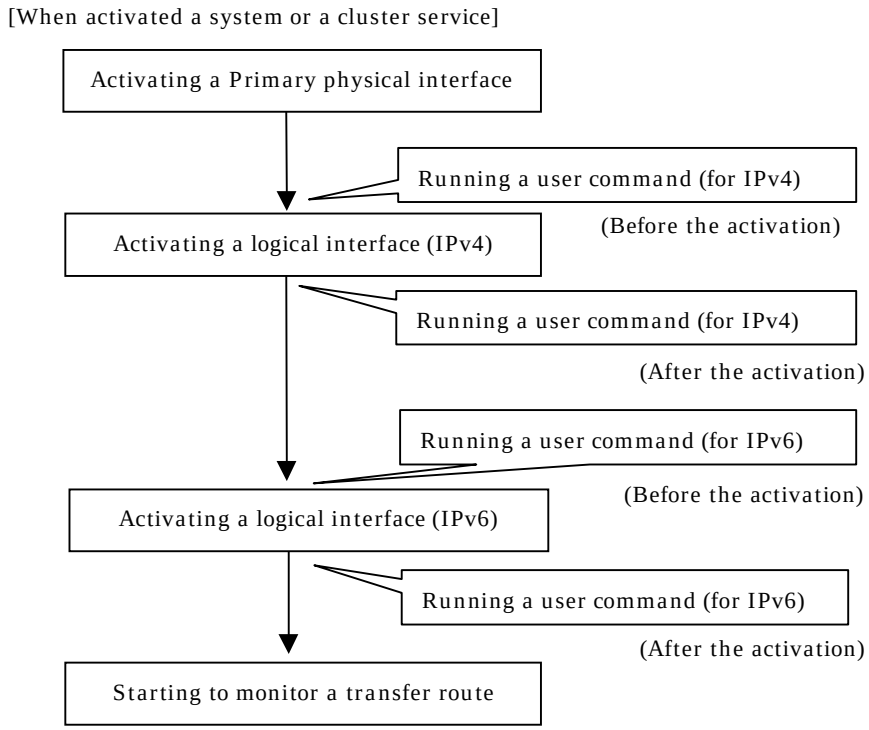


Figure 2.41 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (Continued.)

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

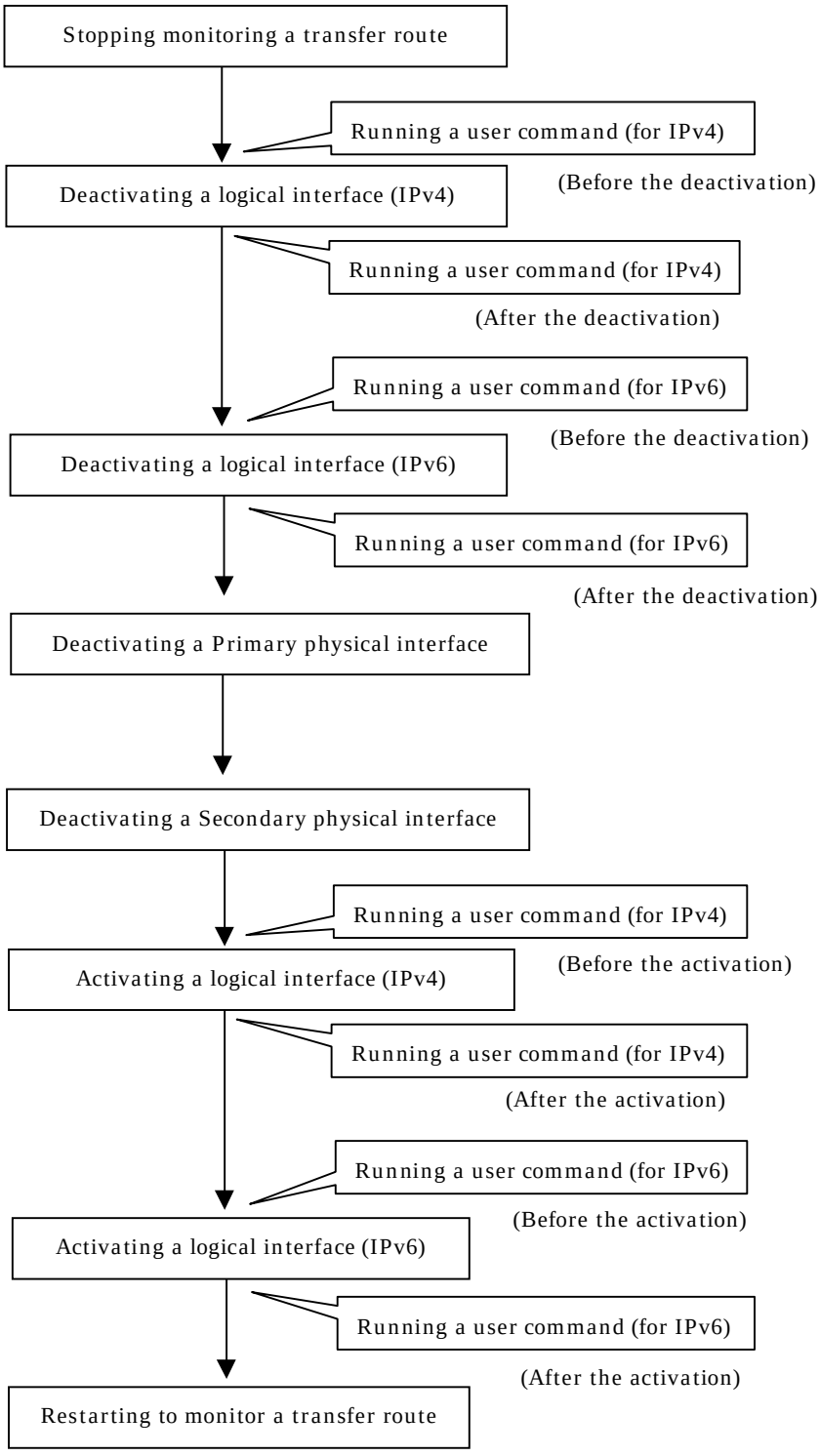


Figure 2.41 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (end.)

Figure 2.42 shows timing to run a user command when activated or deactivated an IP address in NIC switching mode (a physical IP address takeover function).

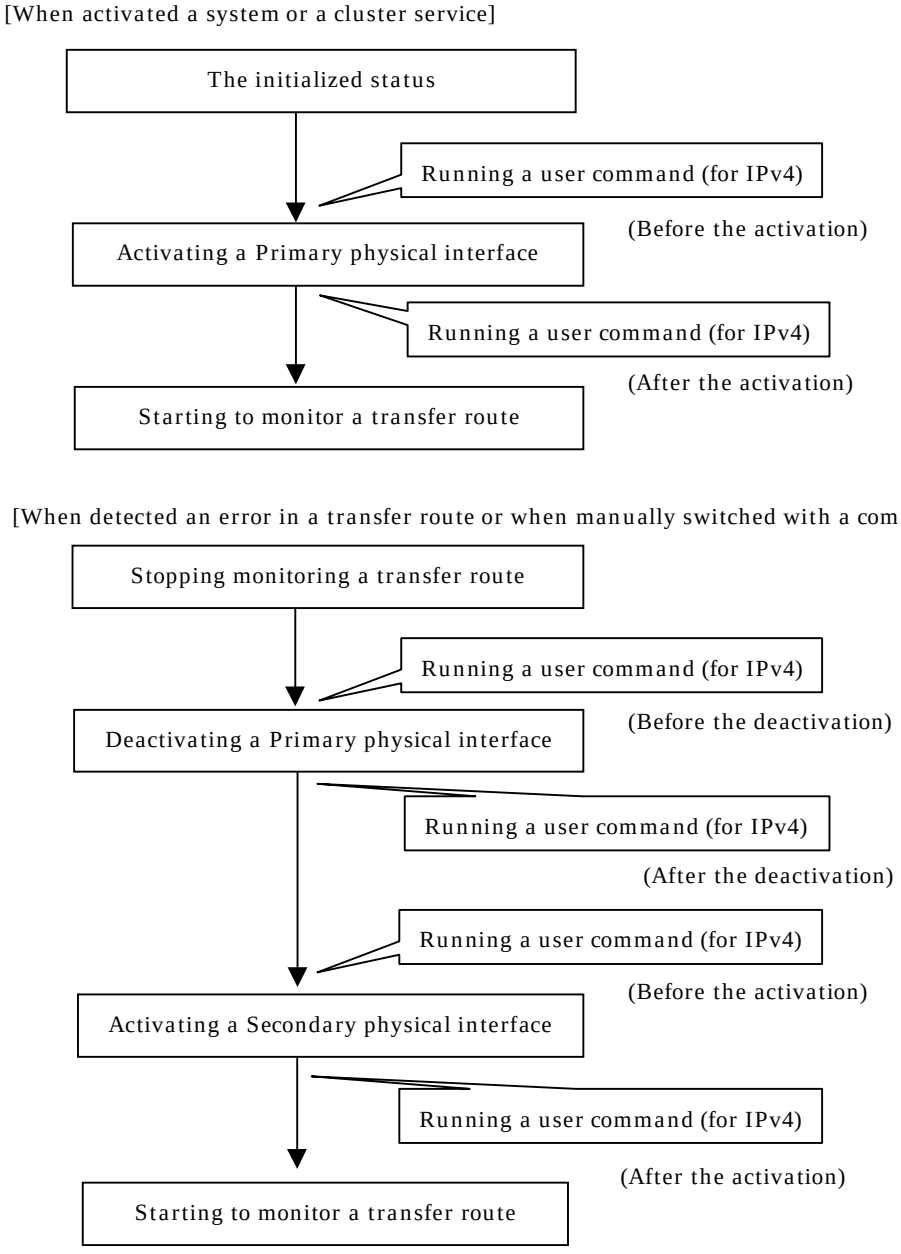
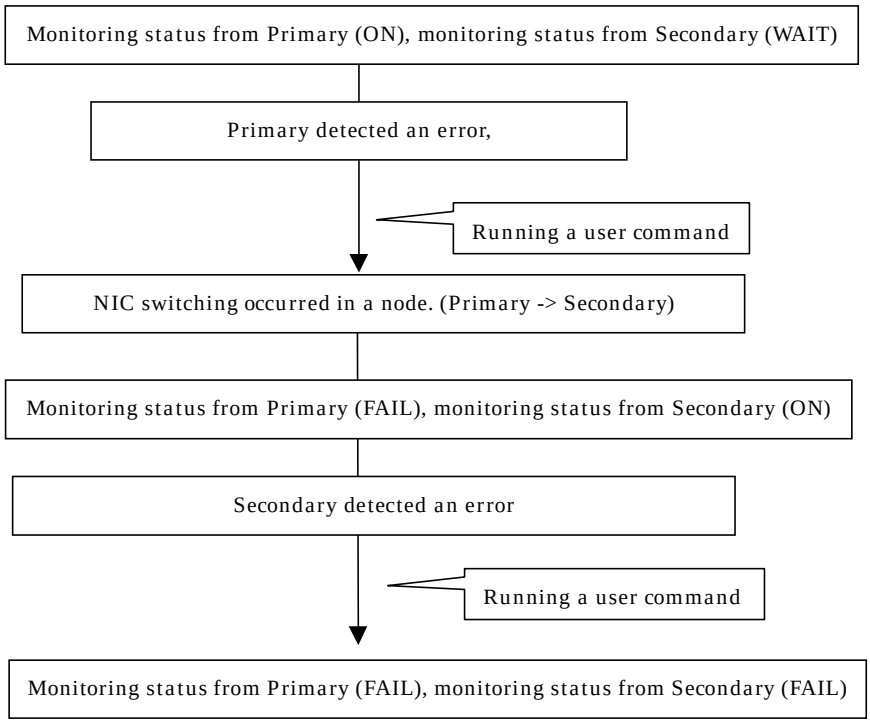


Figure 2.42 Timing of running a user command when activating or deactivating an IP address (a physical IP address takeover function)

Figure 2.43 shows timing to run a user command when detected an error in a transfer route in NIC switching mode

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



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

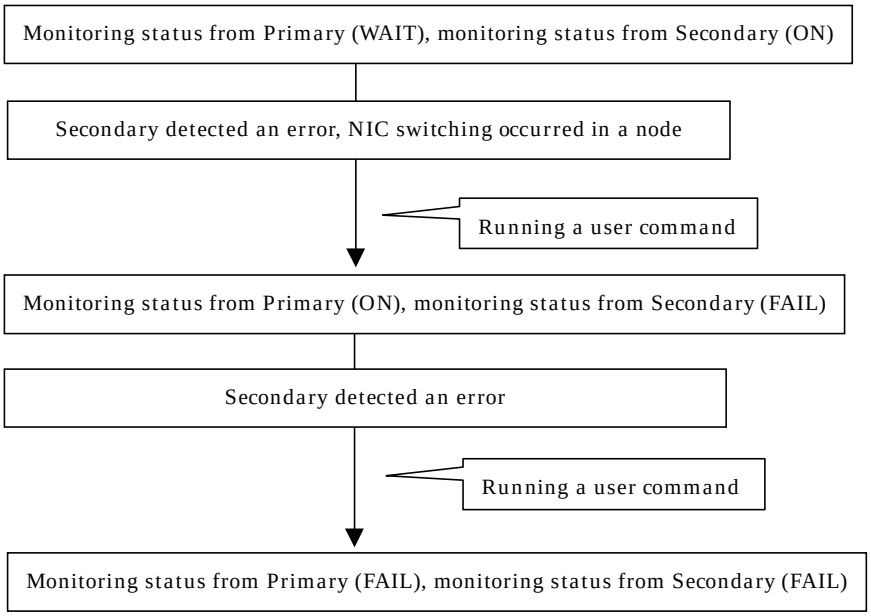


Figure 2.43 Timing of running a user command when detected an error in a transfer route

Figure 2.44 shows timing to run a user command when detected a standby patrol error or recovery in NIC switching mode.

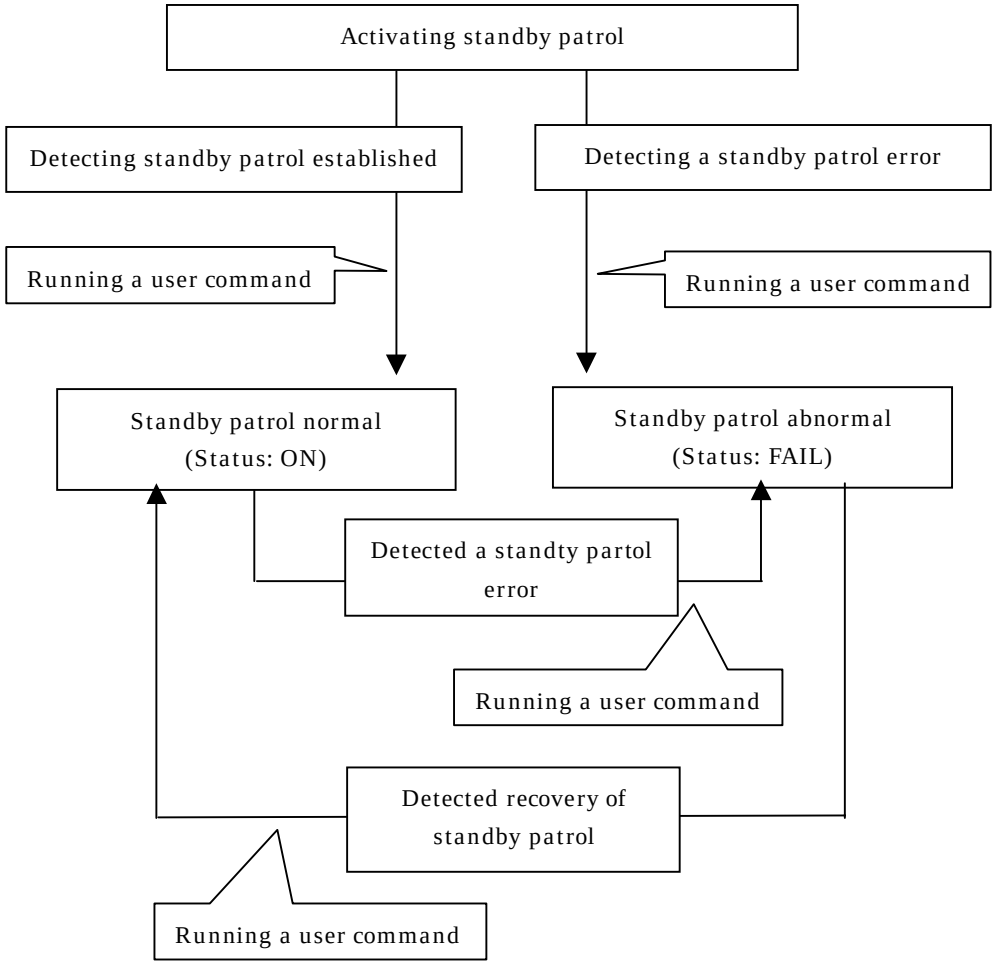


Figure 2.44 Timing of running a user command when detected a standby patrol error or recovery

(2) GS/SURE linkage mode

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

Figure 2.45 shows timing to run a user command when the other system hot standby switched in GS/SURE linkage mode.

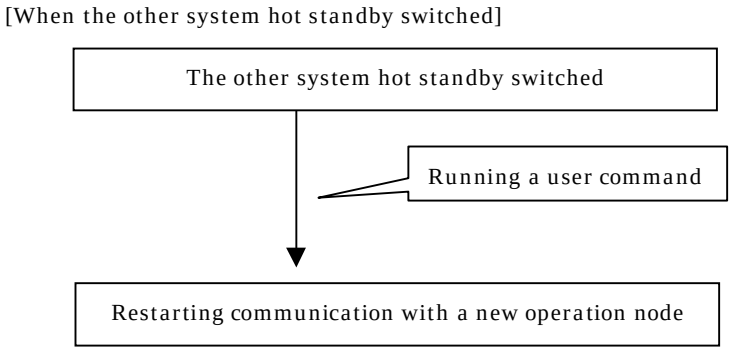


Figure 2.45 Timing of running a user command when the other system hot standby switched

2.3 Other functions

Each mode supports the features shown in the table 2.2.

Table 2.2 Functions available for each mode

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

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

2.3.1 Message output when a line failure occurs

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

2.3.2 DR (Dynamic Reconfiguration) linkage

It is possible to use a DR (Dynamic Reconfiguration) function ("a DR function") provided by PRIMEPOWER 800/900/1000/1500/2000/2500 and GP7000F M1000/2000.

However, it is not possible to use this DR function when defined IPv6 to a virtual interface in Fast switching mode or NIC switching mode.)

See the following manuals to use a DR function.

- Dynamic Reconfiguration User's Guide
- Dynamic Reconfiguration User's Guide I/O device edition

A DR connection script is provided to realize DR in a Redundant Line Control function. Therefore, a DR connection script is invoked by executing a DR command, and it disconnects or connects a virtual interface (sha0, etc.) and an actual interface (hme0, etc.). This makes it possible to execute a DR function without realizing an interface, a function, and a DR connection script used in various modes. "Figure 2.46 The outline of the workings of DR" shows a flow of exchanging system boards (SB) using a DR function.

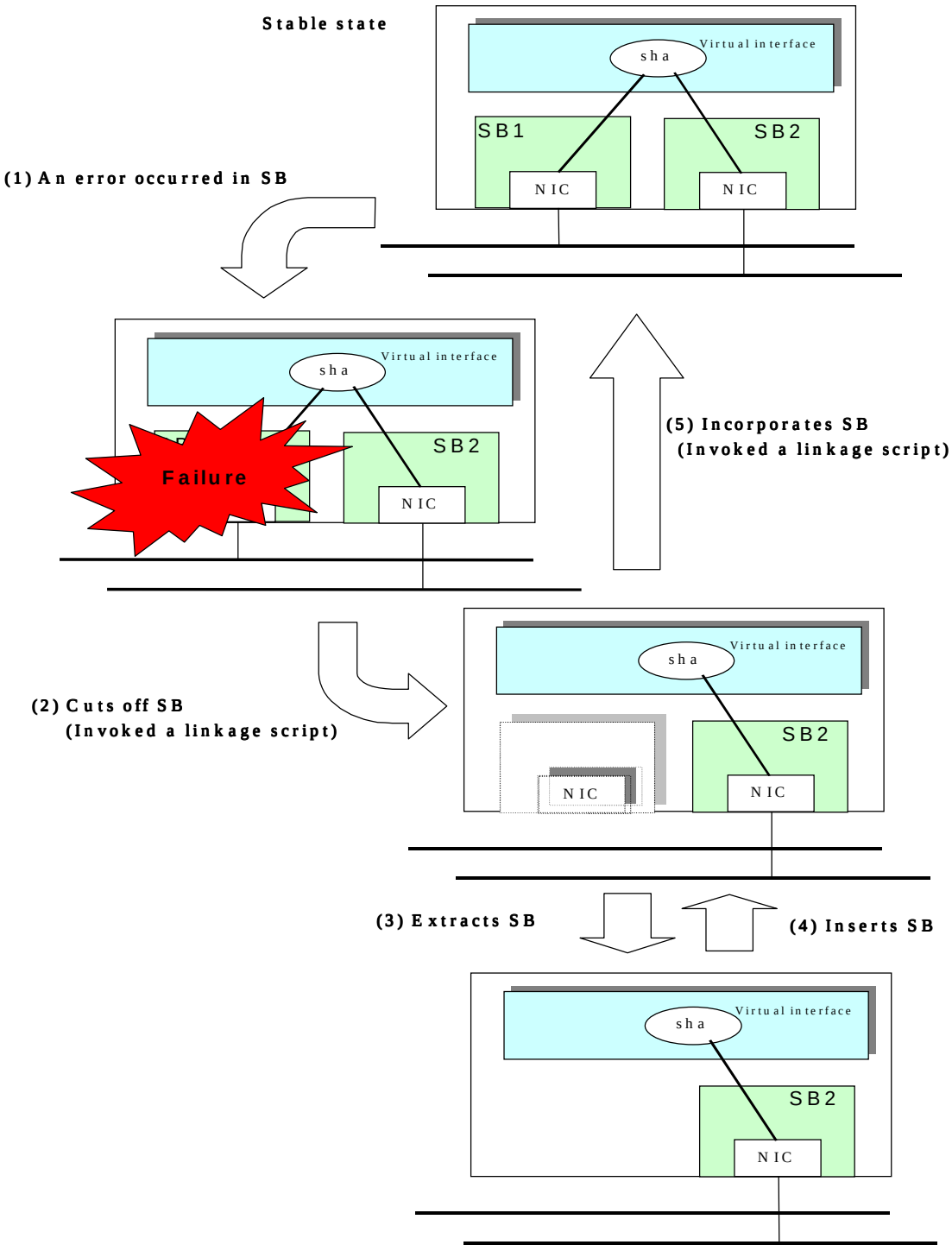


Figure 2.46 The outline of the workings of DR

2.3.3 PCI Hot Plug (PHP) linkage

It is possible to use PCI Hot Plug (PHP) function supported in PRIMEPOWER 450/900/1500/2500/HPC2500.

See the following manuals to use a PHP.

- PCI Hot Plug User's Guide
- PCI Hot Plug User's Guide I/O device edition

Refer to ”4.5.2 Replacement/Expansion PHP (PCI Hot Plug)” for details on PHP.

2.3.4 Interface status monitoring feature

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

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

Table 2.3 Recoverable interfaces using interface status monitoring feature

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

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

2.3.5 Multiplexing transfer route with Tagged VLAN interfaces

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

The figure below shows the network structure that uses Tagged VLAN

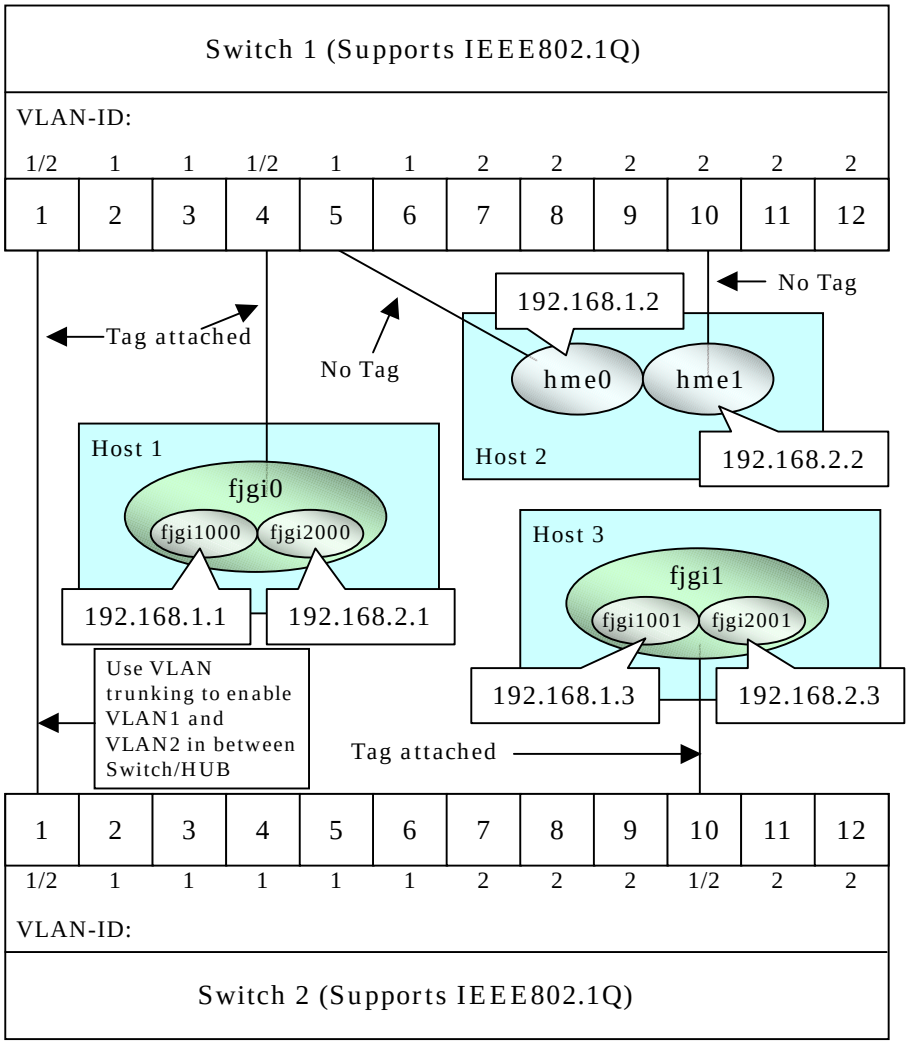


Figure 2.47 Network structure using Tagged VLAN

In Figure 2.47, VLAN1(VLAN-ID:1) and VLAN2(VLAN-ID:2) are created on both Switch 1 and Switch 2, and port1 on both switches is used for VLAN Trunking.
A physical interface "fjgi0" on Host 1 has two VLAN interfaces "figi1000" and "fjgi2000", and is connected to port 4 on Switch 1 that belongs to both VLAN1 and VLAN2. Host 1 uses "fjgi1000" and "fjgi2000" to transmit tagged frames.
Similarly, a physical interface "fjgi1"on Host 3 has two VLAN interfaces "fjgi1001" and "fjgi2001", and is connected to port 10 on Switch 2 that belongs to both VLAN1 and VLAN2. Host 3 uses these VLAN interfaces to establish tagged frame communication.
Host 2 achieves data communications on both VLAN1 and VLAN2 by connecting a physical interface "hme0" to port 5 that belongs to VLAN1, and another physical interface "hme1" to port 10 that belongs to VLAN2.

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

2.3.5.1 Redundant Line Control function using Tagged VLAN interface

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

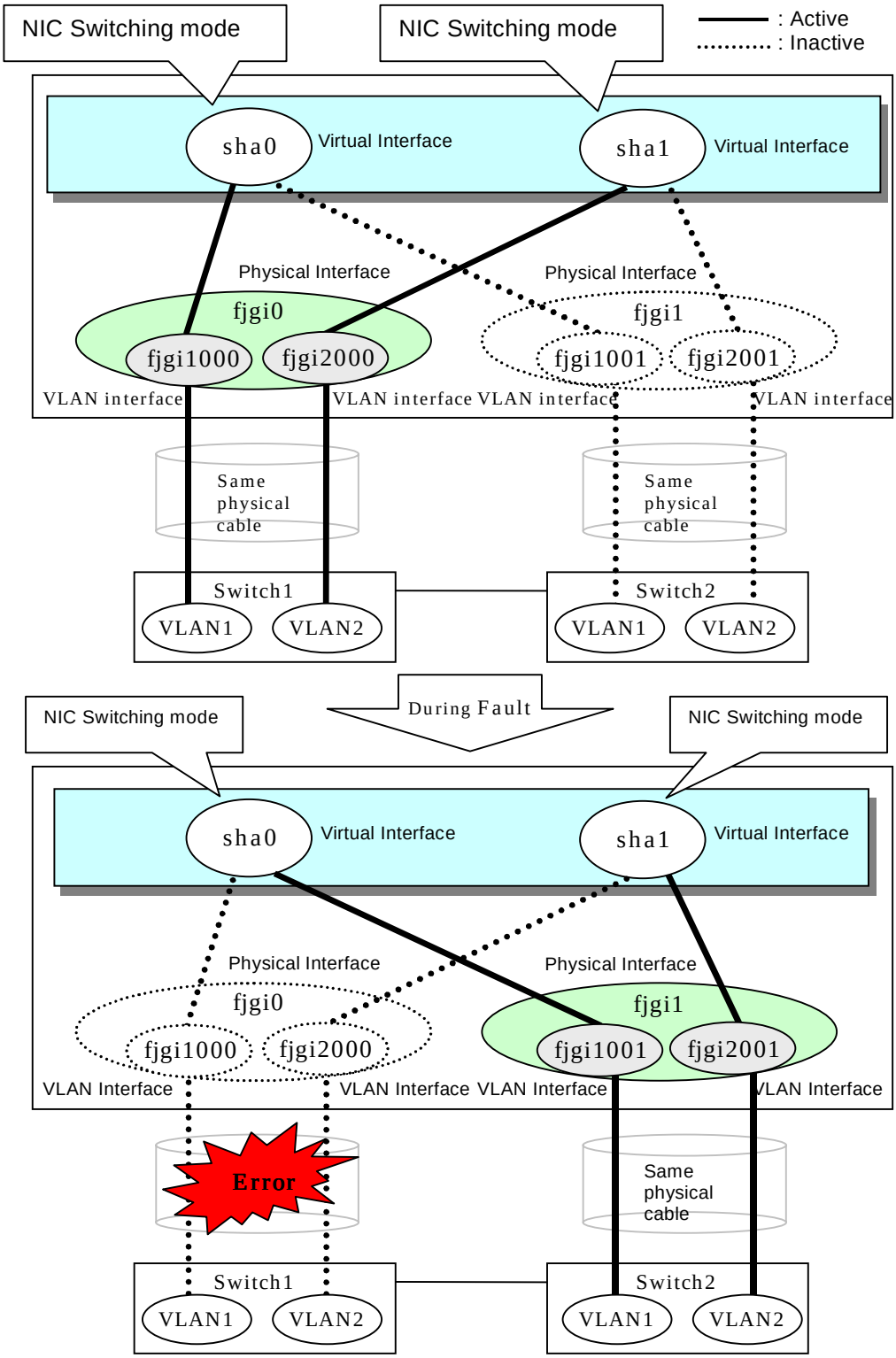


Figure 2.48 Using Tagged VLAN Interface architecture

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.

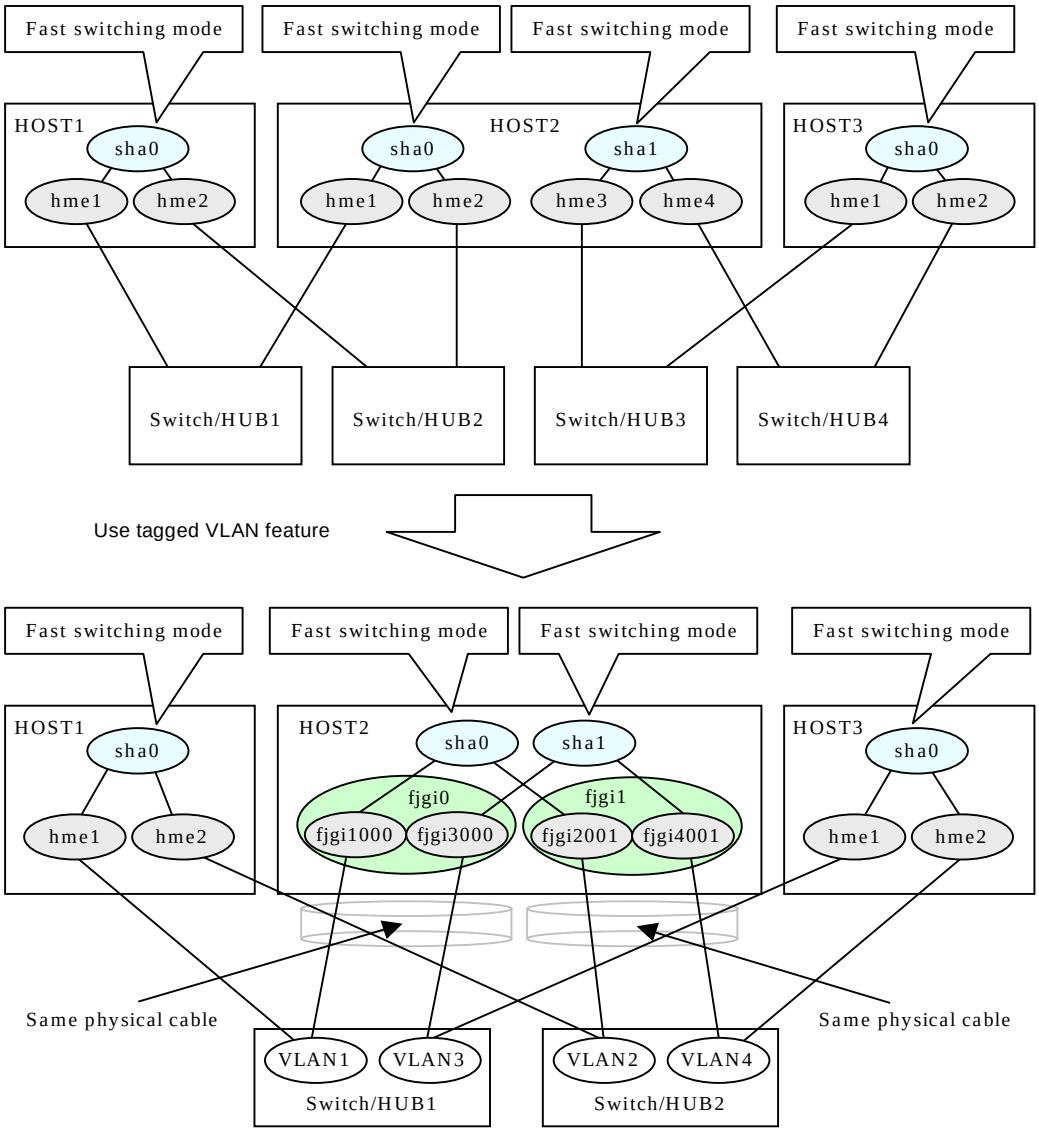


Figure 2.49 When Switch/HUB and NIC come short.

The following modes support a Tagged VLAN.

- Fast switching mode
- NIC switching mode

Multiplexed transfer routes with Tagged VLAN cannot be used in RIP and GS/SURE linkage modes.

For details on using Tagged VLAN for other modes, refer to "3.7.3 Multiplex transfer route using Tagged VLAN Interface".

2.3.6 Line control of Solaris container

Solaris container

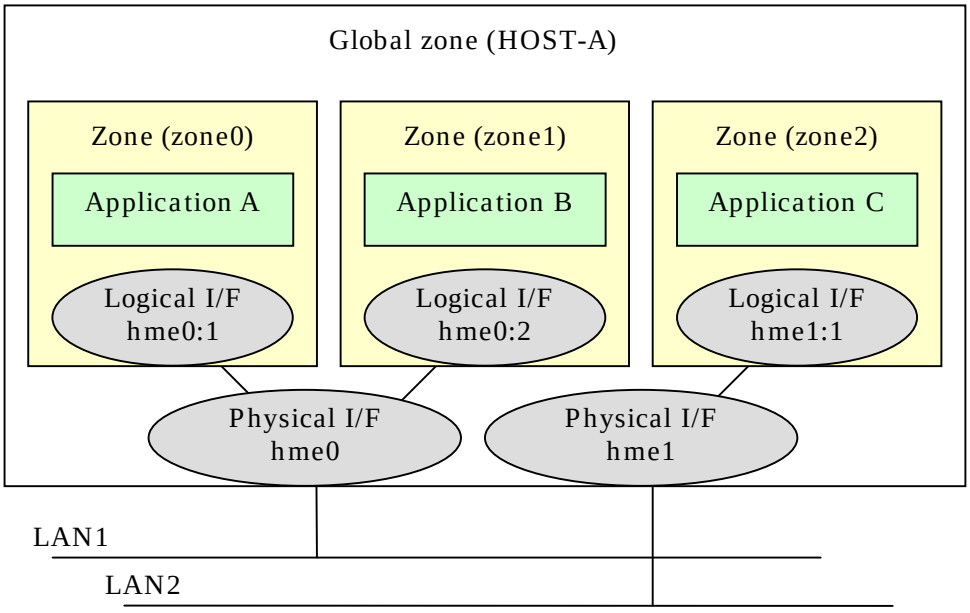
Solaris containers are location independent and complete runtime environments for applications. Each application runs in its own private environment -- without dedicating new systems -- and many applications can be tested and deployed on a single server. Solaris Zones software partitioning technology provides a virtual mapping from the application to the platform resources. Zones allow application components to be isolated from one another even though the zones share a single instance of the Solaris Operating System. The Solaris Zones partitioning technology is used to virtualize operating system services and provide an isolated and secure environment for running applications. A zone is a virtualized operating system environment created within a single instance of the Solaris Operating System.

The virtual server is referred to simply as non-global zone (hereafter, zone). Every Solaris system contains a global zone. The global zone is both the default zone for the system and the zone used for system-wide administrative control. The redundant line control function ensures network high-reliaiblity on the zone.

Network interface of Solaris container

One or more IP address is allocated to each zone of the Solaris container. The IP addresses are added to the logical interface generated on the physical interface. The logical interface is hidden from the other zones, so applications can only use the IP addresses (logical interface) allocated to the zone.

The following figure shows the network interfaces configuration example.



Fugure 2.50 Network interfaces configuration example

Starting each zone from the system (global zone) will enable the zone.

IP addersses (logical interfaces) allocated to each zone are created or deleted from Solaris OS along with zone startup or stop. If physical interfaces or virtual interfaces do not exist, the zone will not be started. If you make the zone network highly reliable through redundant line control, it is necessary to activate the virtual interface before zone startup. However, the redundant line control function will be first started during system startup, so users do not have to be aware of the startup order.

Redundnat line control in Solaris container

The following table describes how each redundant line control function corresponds to high-reliability and GLS command capability in the global or non-global zne of the Solaris container.

Table 2.4 Redundnat line control in Solaris container

Redundant line control		Solaris container			
		Global zone		Non-global zone	
		High-reliablity	GLS command	High-reliablity	GLS command
Fast switching mode	IPv4	Possible	Possible	Possible	Not possible
	IPv6	Possible	Possible	Possible	Not possible
	Dual	Possible	Possible	Possible	Not possible
RIP mode	IPv4	Possible	Possible	Not possible	Not possible
Fast switching / RIP mode	IPv4	Possible	Possible	Not possible	Not possible
NIC switching mode (Logical IP takeover)	IPv4	Possible	Possible	Not recommended	Not possible
	IPv6	Possible	Possible	Possible	Not possible
	Dual	Possible	Possible	Possible	Not possible
NIC switching mode (Physical IP takeover)	IPv4	Possible	Possible	Possible	Not possible
GS/SURE linkage mode	IPv4	Possible	Possible	Not possible	Not possible

- When you make the zone network highly reliable through NIC switching, use physical IP takelover (operation mode "e"). If you use logical iP takeover (operation mode "d"), the redundant line control function will activate a logical IP address as a takeover IP address as well as Solaris OS will activate another logical IP address during zone startop, which means the unnecessary IP address not used by the zone will be activated. If you add the zone settings after setting logical IP takeover (operation mode "d"), it is not necessary to change it to physical IP takeover (operation mode "e").
- The virtal iP address, logical IP address, and physical IP addess allocated through redundant line control can be used in the global zone only. Solaris OS will allocate IP addresses to the non-global zone during zone startup.

The following example shows how to configure the virtual and physical interfaces in fast switching mode.

The application in each zone communicates with each other using the logical/virtual interfaces that are allocated to the virtual interface. Even though an error occurs in the transmission route of the redundant physcail interface (hme0 or hme1), it will never disrupt ongoing operations.

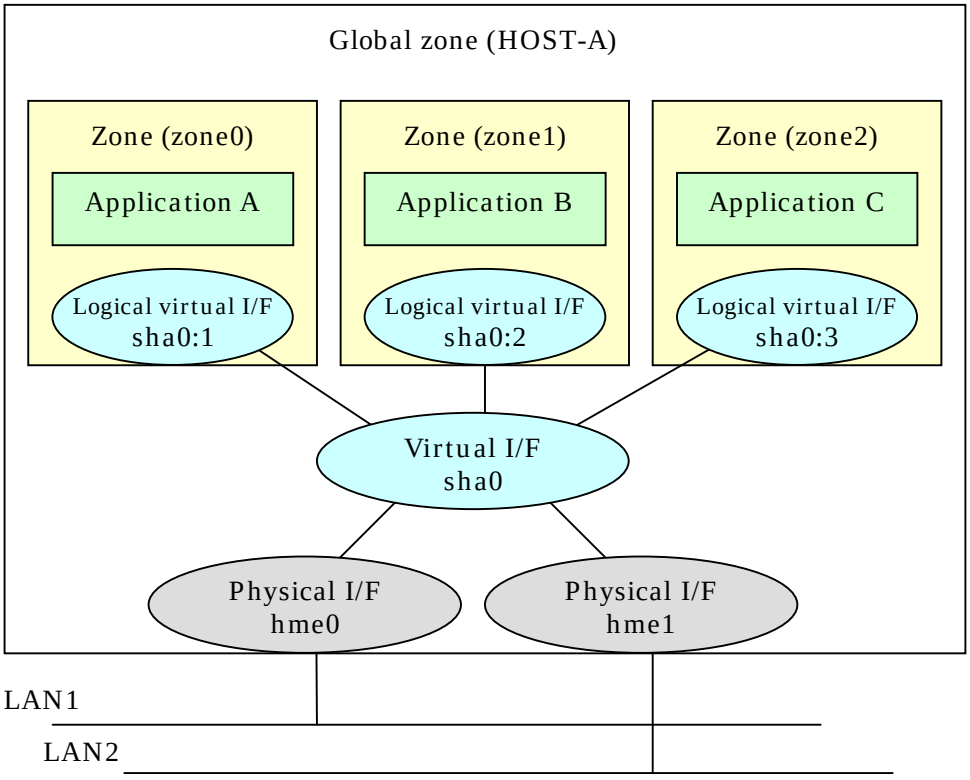


Figure 2.51 Interface structure in fast switching mode

The following example shows how to configure the virtual and physical interfaces in NIC switching mode.

The application in each zone communicates with each other using the logical interfaces that are allocated to the physical interfaces. Even though an error occurs in the transmission route of the redundant physcail interface (hme0), the applications will be switched over to the standby interface (Ihme1) and ensures operational continuity.

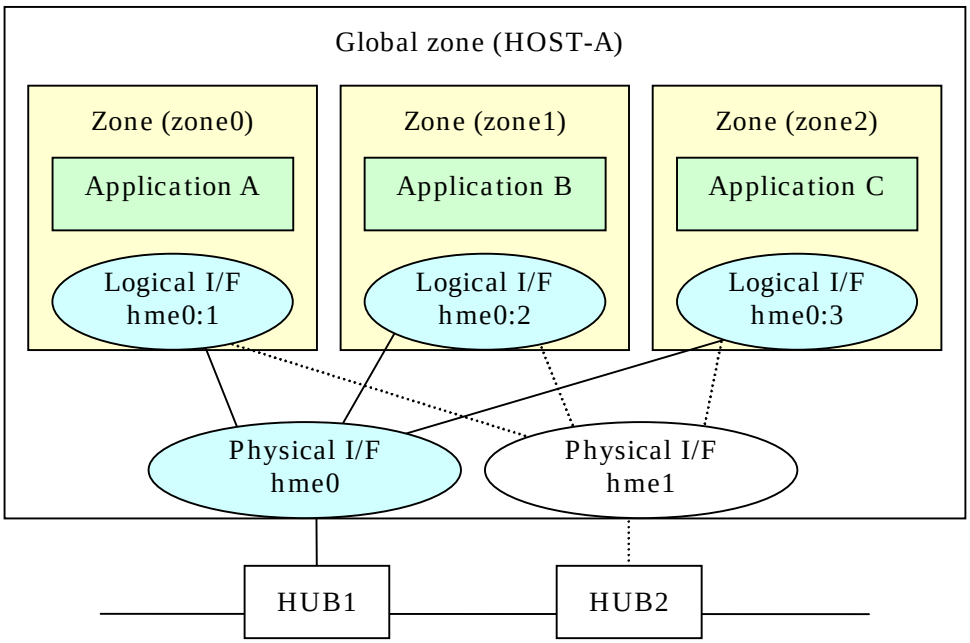


Figure 2.52 Interface structure in fast switching mode

For details about the Solaris container, see the Solris 10 OS manual.

2.3.6.1 Network high-reliability through redundant line control

Normally, the Solaris zones communicate with each other or the other systems by using the logical interfaces of the global zone that is allocated to the physical interface. If the physical interface fials, or part of the transmission route fails, communicatil wil be disrupted.

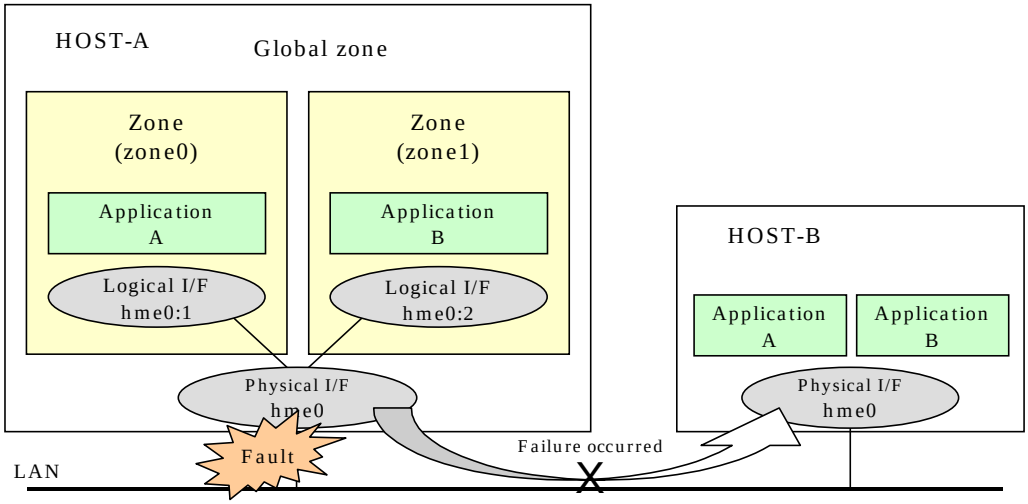


Figure 2.53 Interface structure without redundant line cotnrol

The above example shows that the Application A and B cannot communicate with each other when the transmission route fails.

The redundant line control function ensures operational continuity in the event of a transmission route failure.

Network high-reliability in fast switching mode

The following example shows how interfaces can be structed in fast switching mode.

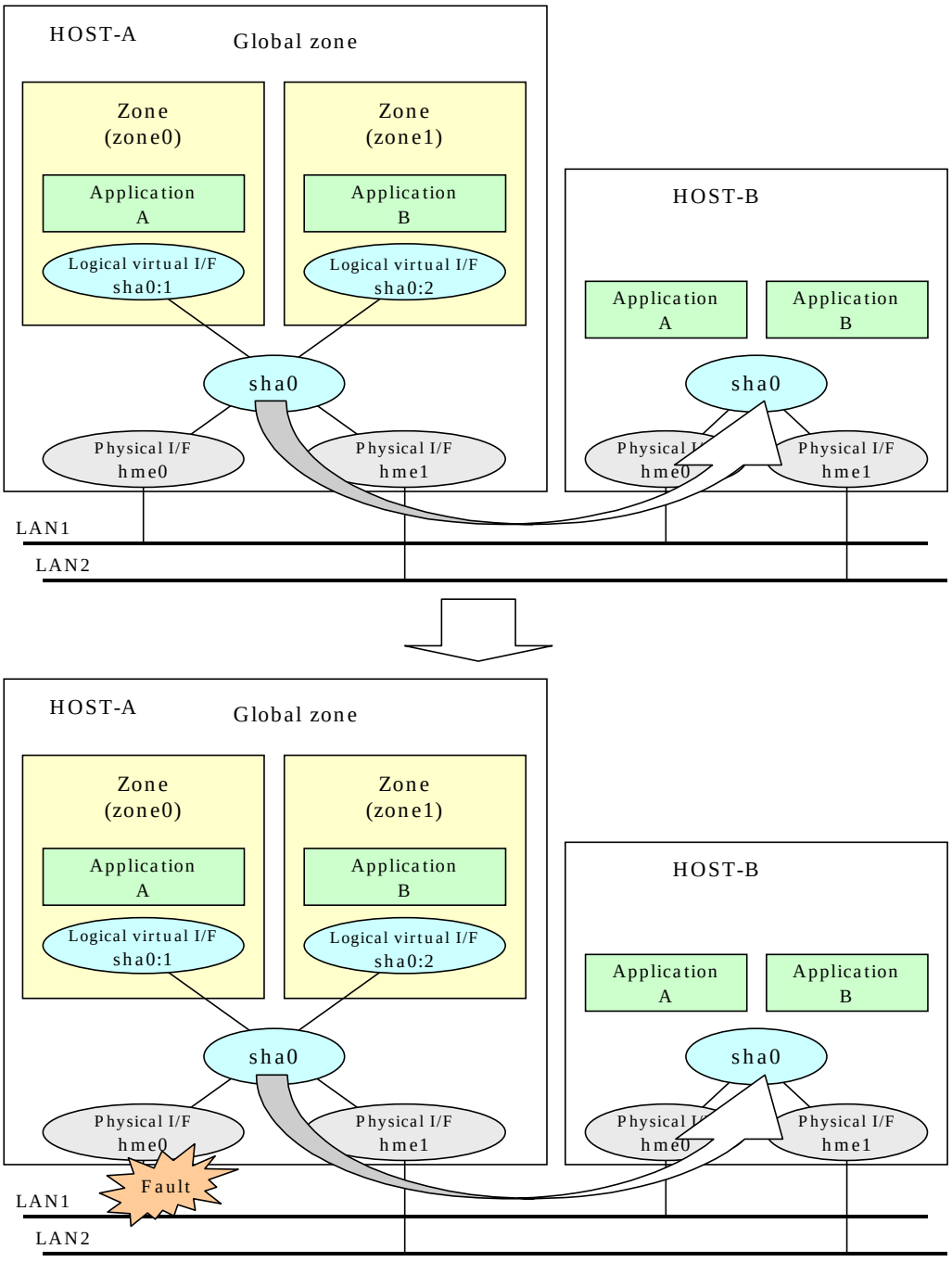


Figure 2.54 Network reliability in fast switching mode

Even if a trousmission route fails on either of the physical interfaces, the applications will be switched over to the logical virtual interface on the standby node through redundant line control, so operational continuity is never disrupted.

Network high-reliability in NIC switching mode

The following example shows how interfaces can be structed in NIC switching mode.

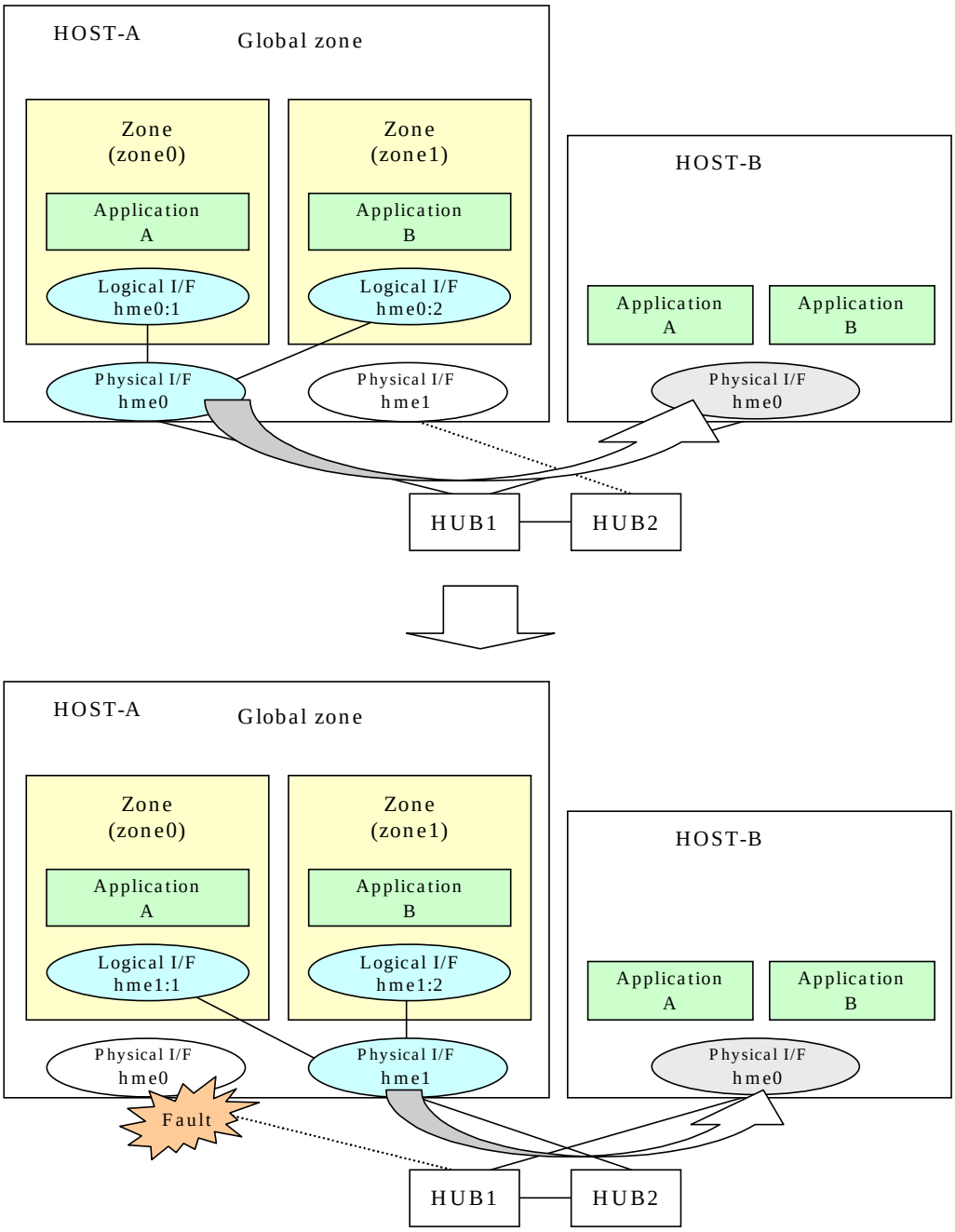


Figure 2.55 Network reliability in NIC switching mode

Even if a trousmission route fails on the primary physical interface, the applications will be switched over to the secondary physical interface through redundant line control, so operational continuity is never disrupted.

2.4 Notes

2.4.1 General

Notes on setting a configuration:

- The minimum and maximum number of virtual and logical virtual interface can be defined is 1 to 64.
- The number of physical interfaces can be used for redundancy on a single virtual interface is within 1 to 8 for Fast switching, RIP, and GS/SURE linkage mode. For NIC switching mode, the range is within 1 to 2.
- The number of logical virtual interfaces that can be defined to a single logical virtual interface is within 1 to 63.
- To use all host names and IP addresses used in a Redundant Line Control function , they must be defined in /etc/inet/ipnodes files of the local system.
- The system automatically determines the length of MTU for an interface. Nonetheless, it is possible to change the length of MTU using user command execution function. For changing MTU length, refer to “3.6.11 Setting user command execution function”. Note that the length of MTU cannot be modified in other redundant modes.

Notes on the operation:

- It is not possible to use a multicast IP address in a Redundant Line Control function.
- Do not execute a DR linkage function in a machine that runs the cluster operation.
- It is not possible to use a Redundant Line Control function under the subnet environment of the variable length. It is not possible to get the route information dynamically under the subnet environment of the variable length because in.routed of Solaris 8 does not support RIP Version2. Set a default gateway and a static route under the subnet environment of the variable length not to activate in.routed. It is not possible to operate under the subnet environment of the variable length in RIP mode and GS/SURE linkage mode because in.routed is used.
- Do not operate physical interfaces that a virtual interface bundles with an ifconfig command.

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, 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. Necessary to execute a recovery process such as sending the data by the application itself.
- It is not possible to use DHCP (a server function and a client function) as the upper application in a Redundant Line Control function.
- 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.

Notes on Solaris container

- If a zone is activated, an interface in the zone cannot be deactivated.
  If you want to change or delete the redundant line control function settings, it is necessary to stop the zone first.
- If a virtual interface does not exist in a zone, the zone cannot be activated.
  Before starting the zone, activate the virtual interface.
- If the zone is started after NIC is switched from the primary interface to the secondary interface in NIC switching mode, it might take up to 20 seconds to enable communication in the zone.
- If the zone is set to use the secondary interface in NIC switching mode, a network

interface in the zone will automatically be swticed to the parimary interface when a virtual interface is activated.

- An IP address specified for a zone and that for a virtual interface must be different. If the same IP is specified for both, zone startup or virtual interface activation will fail.

2.4.2 Duplicated operation by Fast switching mode

- Redundant Line Control function must be operating on each system that performs duplicated operation by Fast switching mode.
- In Fast switching mode, one virtual network is configured to the redundant transfer route. Therefore, a new network number or a 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 to stop using VLAN or to change the setting of VLAN so that it becomes possible to use an optional Ethernet frame.

2.4.3 Duplicated operation by RIP mode

- For duplicated operation by RIP mode, a pair of network interfaces must be connected through at least one router.
- If a fault occurs on an inter-system path during duplicated operation by RIP mode, it takes time to modify the path information between routers (about 5 minutes if the router monitoring function is not enabled, or 1 to 5 minutes if the function is enabled). If the TCP connection is reset during this period, reconnect for recovery from the fault.
- When setting a router (LR) for duplicated operation by RIP mode, the metric value of the network path must be different for each network.
- To configure one virtual network to the redundant transfer route, a new network number is necessary to this virtual network.
- Only one NIC interface is connectable on one network. It is not possible to connect more than one interface on the same network.
- When more than one server sends RIP, occasionally transferring of the route information becomes complicated and takes longer than expected. Therefore, have only one machine to work in RIP mode on the same network.

2.4.4 Duplicated operation by Fast switching/RIP mode

- It is not possible to define more than one virtual interface of Fast switching/RIP mode on the same network. It might not be able to communicate normally.

2.4.5 Duplicated operation via NIC switching mode

- One unit of HUB to be connected in NIC switching mode is sufficient, but communication may not be conducted normally if the HUB has MAC learning capabilities. In such a case, add a HUB to make a HUB-to-HUB connection and then connect the cable to each HUB (See "Figure 2.12 System configuration in NIC switching mode" of "2.1.3 NIC switching mode").
- It is not possible to use a standby patrol function when the type of interface to use is "mpnetX (a logical interface of a multipath)".
- Communication with a multicast IP address is executed using a physical interface (normally, hme0) corresponding to a node name (uname -n). When used this interface in NIC switching mode, it is not possible to communicate with a multicast IP address. This occasionally outputs a following WARNING message from in.rdisc when activated a system:
  in.rdiscd[xxx]: setsockopt(IP_DROP_MEMBERSHIP): Cannot assign requested address
  In this case, either to set /etc/defaultrouter not to activate in.rdisc or reassign a node name to another interface.
- In a standby patrol function of NIC switching mode, a dedicated Ethernet frame is used. Therefore, when operating VLAN (Virtual LAN), occasionally it is not possible to use a standby patrol function depending on the setting of VLAN. In such a case, either to stop

a standby patrol function or VLAN, or change the setting of VLAN so that it becomes possible to use an optional Ethernet frame.

- In NIC switching mode, it is necessary to use a hub that can be assigned an IP address in order for the hub to be monitored. If a hub cannot be assigned an IP address, an IP address of a device connected to the hub can be monitored. However, it should be noted that if the device whose IP address is monitored fails, the failure is regarded as a transfer route failure.
- When using an IPv6 virtual interface, create an /etc/hostname6.interface file corresponding to a Primary physical interface so that an in.ndpd daemon is activated at activating a system. When the in.ndpd daemon is not activated, an IPv6 address is not configured automatically. When creating a /etc/hostname6.interface file, make it empty without fail.
- When using an IPv6 virtual interface, an in.ndpd daemon is occasionally reactivated not to delay configuring an IPv6 address automatically. A message "SIGHUP: restart and reread config file" is output from the in.ndpd daemon following this, but this is not an error.

2.4.6 Duplicated operation via GS/SURE linkage mode

- In GS/SURE linkage mode, the system uses duplicated paths concurrently but it cannot be expected to improve the throughput.
- Be sure to set a function to monitor the other side to communicate when using GS/SURE linkage mode. See "7.5 hanetobserv Command" as to how to set.
- GS/SURE linkage mode and RIP mode cannot be coexisted on a single system.
- In GS/SURE mode, data communication with PRIMEPOWER or GP7000F sever is not possible.
- When switched a cluster on the PRIMEPOWER, GP7000F side, it is possible to recover the communication immediately on the Global Server and PRIMEPOFORCE side because TCP connection is forcibly released. However, when switched a hot standby at the global server and PRIMEPOFORCE side, TCP connection is not forcibly released at the PRIMEPOWER, GP7000F side. Therefore, it is necessary to recover the communication by forcibly releasing each TCP application.

Chapter 3 Environment configuration

This chapter discusses how to set up and configure GLS.

3.1 Setup

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

The following is the procedure of this configuration

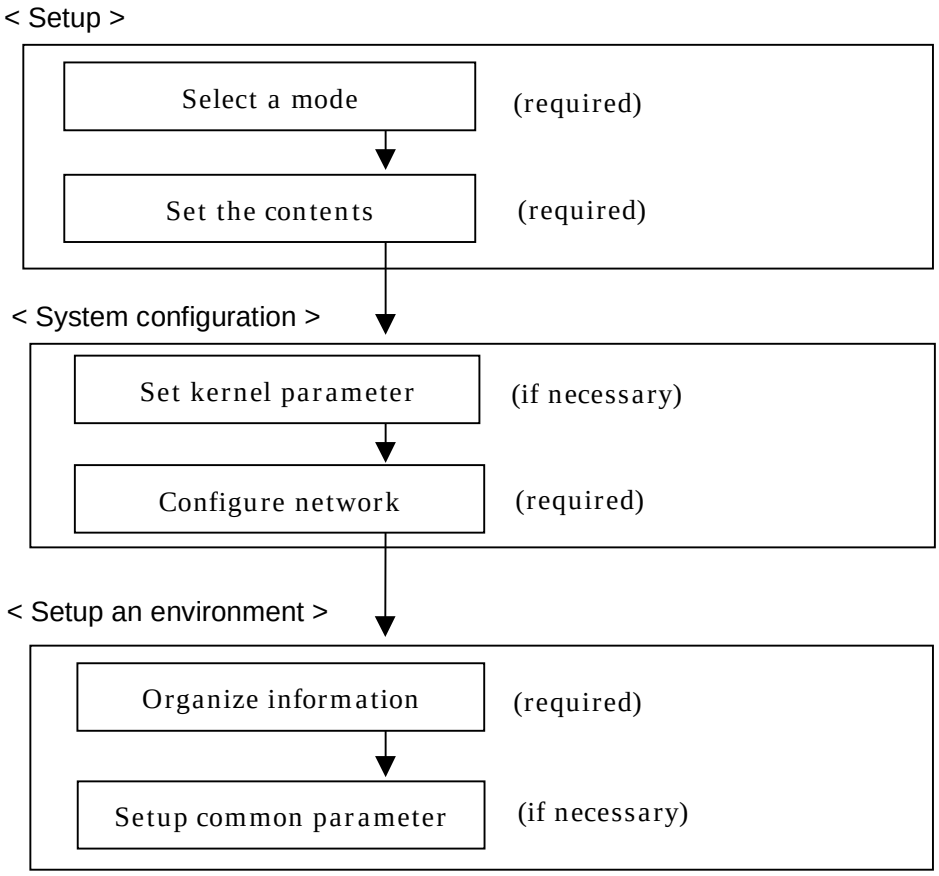


Figure 3.1 Configuration to Setting up an environment

3.1.1 Selecting mode

Determine which mode to use. Table 3.1 indicates the selection of modes.

For selecting adequate mode, refer to “1.1.2 Selecting mode”.

Table 3.1 Selection of modes

Mode	Selecting mode
Fast switching mode	Select this mode if every one of the remote hosts is a Solaris server or Linux server. This mode can detect the abnormalities of the multiplexed transfer route immediately. When abnormalities are detected, communication can be immediately changed to a normal transfer route.
RIP mode	Select this mode if communicating with server over the other network and attempting to switch over using RIP standard protocol. Usually, this mode is not used
Fast switching/ RIP mode	Select this mode if using a single virtual interface in Fast switching mode and RIP mode at the same time.
NIC switching mode	Select this mode, if a hot-standby router, a network load balancer, or servers and other various network devices from other manufacturers are used. Select this mode in most cases.
GS/SURE linkage mode	Select this mode if using GS and SURE SYSTEM exclusively. Other servers or any network device must not exist in the same network.

It is possible to create multiple virtual interfaces in a single system to use several modes concurrently, though it is not possible to use RIP mode and GS/SURE linkage mode together.

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

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

3.1.2 Selecting appropriate contents

Select appropriate contents for each mode.

3.1.2.1 Fast switching mode

When using Fast switching mode, determine the information required for configuration of the mode listed in the table 3.2.

Table 3.2 Configuration information of Fast switching mode

Components			Values
Virtual interface information (1)	Virtual interface name		T-1
	Virtual IP address or host name		T-2
	Subnet mask		T-3
	Physical interface information (1)	Physical interface name	T-4
		IP address or host name	T-5
		Subnet mask	T-6
	Physical interface information (2)	Physical interface name	T-7
		IP address or host name	T-8
		Subnet mask	T-9
	(Repeat for the number of physical interfaces)		
(Repeat for the number of virtual interfaces)			

Description of each component is as follows:

<Virtual interface information>

Setup the followings for the number of virtual interfaces.

Virtual interface name(T-1)

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(T-2)

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

Subnet mask(T-3)

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

<Physical interface information>

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

Physical interface name(T-4,7)

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

Physical IP address or host name(T-5,8)

If using IPv4 address, specify an IP address or host name to be assigned for the physical interface. The network portion of this IP address must be different from IP address of other physical and virtual interface. To setup this component, create "/etc/hostname.*physical interface name*" file and then assign the IP address (or host name) in the file.
Make sure this value is different from the other IP.

Subnet mask (T-6,9)

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

3.1.2.2 RIP mode

When using RIP mode, determine the information required for the configuration listed in the table 3.3.

Table 3.3 Configuration information of RIP mode

<table>
<tr><th colspan="3">Components</th><th>Values</th></tr>
<tr><td rowspan="11">Virtual interface information (1)</td><td colspan="2">Virtual interface name</td><td>R-1</td></tr>
<tr><td colspan="2">Virtual IP address or host name</td><td>R-2</td></tr>
<tr><td colspan="2">Subnet mask</td><td>R-3</td></tr>
<tr><td rowspan="3">Physical interface information (1)</td><td>Physical interface name</td><td>R-4</td></tr>
<tr><td>IP address or host name</td><td>R-5</td></tr>
<tr><td>Subnet mask</td><td>R-6</td></tr>
<tr><td rowspan="3">Physical interface information (2)</td><td>Physical interface name</td><td>R-7</td></tr>
<tr><td>IP address or host name</td><td>R-8</td></tr>
<tr><td>Subnet mask</td><td>R-9</td></tr>
<tr><td colspan="3">(Repeat above entries for the number of physical interfaces)</td></tr>
<tr><td rowspan="2">Monitored remote system information</td><td>Primary Monitored remote system IP address or host name</td><td>R-10</td></tr>
<tr><td>Secondary Monitored remote system IP address or host name</td><td>R-11</td></tr>
<tr><td colspan="4">(Repeat above entries for the number of virtual interfaces)</td></tr>
</table>

Description of each component is as follows:

<Virtual interface information>

Setup the followings for the number of virtual interfaces.

Virtual interface name (R-1)

Specify a name of the virtual interface assigned to a physical interface for redundancy. Specify shaX (X represents a number) of this component using “hanetconfig create” command with -n option.

Virtual IP address or host name (R-2)

Specify an IPv4 address or host name to be assigned for the virtual interface. The network portion of this IP address must be different from an IP address allocated for the physical interface. Specify this entry using “hanetconfig create” command with -i option.

Subnet mask (R-3)

Specify the value of sub network mask applied to the virtual IP address. Configuration can be omitted if not allocating subnet. Describe this entry in /etc/inet/netmasks file. If subnet mask is applied, use the same mask value for the whole virtual IP and physical IP.

<Physical interface information>

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

Physical interface name (R-4,7)

Specify the name of physical interface. This can be setup using “hanetconfig create” command with -t option. (e.g. hme1,qfe2, etc)

Physical IP address or host name (R-5, 8)

If using IPv4 address, specify an IP address or host name to be allocated for the physical interface. The network portion of this IP address must be different from IP address of other physical and virtual interfaces. In order to specify the physical IP address, create “/etc/hostname.<physical interface name>" file and then specify IP address (or host name) in the file.
Make sure this value is different from the other IP.

Subnet mask (R-6, 9)

Specify the value of sub network mask applied to the virtual IP address. This configuration can be omitted if not allocating a subnet. Write this entry in /etc/inet/netmasks file. When applying subnet mask, apply the same mask value to a whole virtual and physical IP.

<Monitored remote system information>

Configure the followings for the number of virtual interfaces. This process can be omitted.

Primary Monitored remote system IP address or host name (R-10)

Specify the IP address (or host name) of the router to be monitored while using the primary physical interface. This entry is specified using “hanetpoll create” command with -p option.

Secondary Monitored remote system IP address or host name (R-11)

Specify an IP address (or host name) of the router to be monitored while using the secondary physical interface. This entry is specified using “hanetpoll create” command with -p option. This process can be omitted. If this process is omitted, the same value as the primary Monitored remote system IP address (or host name) will be applied.

3.1.2.3 Fast switching/RIP mode

If using Fast switching/RIP mode, see “3.1.2.1 Fast switching mode” and “3.1.2.2 RIP mode”.

3.1.2.4 NIC switching mode

Table 3.4 shows the information required to configure NIC switching mode:

Table 3.4 Configuration information of NIC switching mode

Components			Values
Virtual interface information (1)	Virtual interface name		D-1
	Virtual IP address (or host name)		D-2
	Subnet mask		D-3
	Physical interface information (1)	Physical interface name	D-4
		IP address or host name	D-5
	Physical interface information (2)	Physical interface name	D-6
	Standby interface information	Virtual interface name	D-7
		Automatic switching back mode	D-8
		Local MAC address configured in Standby interface	D-9
	Monitored remote system information	Primary Monitored remote system IP address or host name	D-10
		Secondary Monitored remote system IP address or host name	D-11
		HUB-to-HUB monitoring	D-12
(Repeat for the number of physical interfaces)			

Description of each component is as follows:

<Virtual interface information>

Setup the followings for the number of virtual interfaces.

Virtual interface name (D-1)

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 (D-2)

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(D-3)

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

<Physical interface information>

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

Physical interface name (D-4,6)

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

Physical IP address or host name (D-5)

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

<Standby patrol information>

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

Virtual interface name (D-7)

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 (D-8)

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

Local MAC address configured in Standby interface (D-9)

If the standby patrol function is used, specify a local MAC address to be allocated to the standby interface. A local MAC address is specified in the form of: "02:XX:XX:XX:XX:XX" (where X represents a hexadecimal digit between 0 and F). The leading value "02" indicates the local MAC address, and the rest of the values can be arbitrary. However, please make sure that each MAC address should be unique within a single network. If the same MAC address is used within a network, the standby patrol may not run properly. A local MAC address is specified using "hanetconfig create" command with -a option.

<Monitored remote system information>

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

Primary Monitored remote system IP address or host name (D-10)

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

Secondary Monitored remote system IP address or host name (D-11)

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

HUB-to-HUB monitoring (D-12)

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

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

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

3.1.2.5 GS/SURE linkage mode

Table 3.5 shows the information required to configure GS/SURE linkage mode.

Table 3.5 Configuration information of GS/SURE linkage mode

<table>
<tr><th colspan="5">Components</th><th>Value</th></tr>
<tr><td rowspan="10">Virtual interface information (1)</td><td colspan="4">Virtual interface name</td><td>C-1</td></tr>
<tr><td colspan="4">Virtual IP address or host name</td><td>C-2</td></tr>
<tr><td colspan="4">Subnet mask</td><td>C-3</td></tr>
<tr><td colspan="2" rowspan="3">Physical interface information (1)</td><td>Physical interface name</td><td>C-4</td></tr>
<tr><td>IP address or host name</td><td>C-5</td></tr>
<tr><td>Subnet mask</td><td>C-6</td></tr>
<tr><td colspan="2" rowspan="3">Physical interface information (2)</td><td>Physical interface name</td><td>C-7</td></tr>
<tr><td>IP address or host name</td><td>C-8</td></tr>
<tr><td>Subnet mask</td><td>C-9</td></tr>
<tr><td colspan="4">(Repeat for the number of the physical interfaces)</td></tr>
<tr><td colspan="6">(Repeat for the number of the virtual interfaces)</td></tr>
<tr><td rowspan="8">Remote node information (1)</td><td colspan="4">Remote node name</td><td>C-10</td></tr>
<tr><td rowspan="6">Virtual IP information (1)</td><td colspan="3">Virtual IP address</td><td>C-11</td></tr>
<tr><td rowspan="3">Remote host physical IP address information</td><td>IP address or host name (1)</td><td>C-12</td></tr>
<tr><td>IP address or host name (2)</td><td>C-13</td></tr>
<tr><td colspan="2">(Repeat for the number of IP addresses)</td></tr>
<tr><td colspan="3">Monitoring on/off</td><td>C-14</td></tr>
<tr><td colspan="3">Send RIP from remote host on/off</td><td>C-15</td></tr>
<tr><td colspan="3">Network information of relaying host</td><td>C-16</td></tr>
<tr><td colspan="4">(Repeat for the number of virtual IP)</td></tr>
<tr><td colspan="6">(Repeat for the number of remote nodes)</td></tr>
</table>

Description of each component is as follows:

<Virtual interface information>

Setup the followings for the number of virtual interfaces.

Virtual interface name (C-1)

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 (C-2)

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 (C-3)

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

<Physical interface information>

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

Physical interface name (C-4,7)

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 (C-5,8)

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

Subnet mask (C-6,9)

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

<Remote node information>

Configure the following for the number of host nodes.

Remote host name (C-10)

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

<Virtual IP information>

Setup the followings for the number of virtual IP.

Virtual IP address or host name (C-11)

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 (C-12,13)

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

Monitoring on/off (C-14)

Set whether or not to use monitoring function.
on: Turn on the monitoring function from the local host
off: Does not turn on the monitoring.
If monitoring is enabled from the remote host, monitoring the remote host can be omitted. Check the configuration of the remote host and decide whether or not to turn on the monitoring function.
If the remote host (GS) is setup as a hot standby server, then define this in either active node or standby node. This configuration can be specified via “hanetobserv create” command with -m option.

Send RIP from remote host on/off (C-15)

For this component, specify whether or not to send RIP packets from a remote host.
on: Awaits notification from the remote host and sends notification of the node whether the node has switched or not. After receiving RIP packets from the remote host, it sends out the notification.
off: Does not wait for notification from the remote host. It sends out a notification to every path.
Initially, this is set to “on”. If the global server (GS) is setup as a hot standby server, then define this in either operation node or standby node while setting up Monitored remote system information. This configuration is specified using “hanetobserv create” command with -r option.
Caution) If the remote system is setup as a hot standby server, because RIP determines whether operational node or standby is functioning, the parameter should be set as “on”.

Network information of relaying host (C-16)

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

3.1.2.6 Configuration of individual mode

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

Table 3.6 Configuration of redundancy mode

Contents	Fast switching mode	RIP mode	Fast switching /RIP mode	NIC switching mode	GS/SURE linkage mode	Value	Default
Transfer path monitoring interval	A	N	A	N	N	K-1	5 sec
The number of constant monitoring prior to outputting message	A	N	A	N	N	K-2	0 time
The number of constant monitoring prior to switching cluster	A	N	A	N	N	K-3	5 sec
Switching cluster immediately after starting	A	N	A	N	N	K-4	none
Outputting message (monitoring the physical interface)	A	N	A	N	N	K-5	none
Standby patrol monitoring period	N	N	N	A	N	K-6	15 sec
The number of constant standby monitoring prior to outputting message	N	N	N	A	N	K-7	3 times
Deactivating the standby interface	N	N	N	A	N	K-8	Inactive
Monitoring period	N	A	A	A	A	K-9	5 sec

The number of monitoring	N	A	A	A	A	K-10	5 times
The number of retries until router monitoring stops	N	A	N	N	N	K-11	5 times
Recovery monitoring period	N	A	A	N	A	K-12	5 sec
Cluster switching	N	A	A	A	A	K-13	Yes
Link up waiting period	N	A	A	A	A	K-14	60 sec

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

The followings are description of each of the content.

Transfer path monitoring interval (K-1)

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. 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 and Fast switching/RIP mode.

The number of constant monitoring prior to message output (K-2)

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

The number of constant monitoring prior to switching cluster (K-3)

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 and Fast switching/RIP mode.

Switching cluster immediately after starting (K-4)

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 and Fast switching/RIP mode.

Outputting message (monitoring the physical interface) (K-5)

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 outputted. If “off” is selected, a message is not outputted. Initially, it is set to “off”. This setting is specified via “hanetparam” command with -s option. This is available for Fast switching and Fast switching/RIP mode.

Standby patrol monitoring period (K-6)

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

The number of constant standby monitoring prior to outputting message (K-7)

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

Deactivating the standby interface (K-8)

Specify how the standby interface is deactivated. The values which can be specified are either “plumb” or “unplumb”. If “plumb” parameter is specified, the standby interface is deactivated and sets “0.0.0.0” for the IP address. With this parameter, it is possible to use “INTERSTAGE Traffic Director” as a high-level application. On the other hand, selecting “unplumb” deactivates the standby interface and then it sets to unused status. Initially, the parameter is set to “unplumb”.
If you make the Solaris container network highly reliable through NIC switching mode, it is necessary to specify "plumb".
This configuration is specified by “hanetparam” command with -d option. This is available exclusively for NIC switching mode.

Monitoring period (K-9)

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

The number of monitoring (K-10)

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

The number of retries until router monitoring stops (K-11)

Specify the number of retries in order to stop monitoring when a failure is detected. The values which can be specified are from 0 to 99999. Initially, the value is set to 5 (times). If not to stop monitoring, set this value to "0". This configuration is specified using “hanetpoll on” command with -r option. This feature is available for RIP, Fast switching/RIP mode.

Recovery monitoring period (K-12)

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

Cluster switching (K-13)

Specify whether or not to switch the node when a failure occurs to every transfer paths.
yes: Switch nodes when a failure occurs to a whole transfer paths.
no: Does not switch nodes when a failure occurs to a whole transfer path.
The default parameter is “yes”. This configuration is specified by “hanetpoll on” command with –f. This feature is available for RIP, Fast switching/RIP, NIC switching, and GS/SURE linkage mode operating as a cluster.

Link up waiting period (K-14)

In NIC switching mode, 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). 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 “hanetpoll on” command with -p option. This feature is available for RIP, Fast switching/RIP, NIC switching and GS/SURE linkage mode.

3.2 System Setup

Setup the system according to the contents determined in “3.1 Setup”.

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

3.2.1 Setup kernel parameters

In Redundant Line Control function, the following values are required for the kernel parameter. If the required value is insufficient in a whole system, then add sufficient values. For modifying the kernel parameter, refer to the Solaris manual.

Table 3.13 Required Kernel parameter

Kernel parameter		Required value	Description
Solaris 8 or Solaris 9	shmsys:shminfo_shmmax	5120 or more	Maximum size of shared memory segment.
	shmsys:shminfo_shmmni	2 or more	Maximum amount of shared memory segment.
	semsys:seminfo_semmni	1 or more	Maximum semaphore identification value
	semsys:seminfo_semmns	1 or more	Maximum semaphore identification value in the system
Solaris 10	project.max-shm-memory	5120 or more	Total number of bites of shared memory
	project.max-shm-ids	2 or more	Total number of identifiers of shared memory
	project.max-sem-ids	1 or more	Total number of semaphores of shared memory

3.2.2 Network configuration

3.2.2.1 Setup common to modes

(1) Verification of the physical interface

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

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

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

```
# prtconf -D | grep qfe
                    SUNW,qfe, instance #0 (driver name: qfe)
                    SUNW,qfe, instance #1 (driver name: qfe)
                    SUNW,qfe, instance #2 (driver name: qfe)
                    SUNW,qfe, instance #3 (driver name: qfe)
```

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

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

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

(2) Checking the name service

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

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

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

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

3.2.2.2 System setup in Fast switching mode

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

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

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

3.2.2.3 System setup in RIP mode

- After configuring a GLS environment, hostname information on a host database (such as /etc/inet/hosts file) should not be modified, if it has been used for GLS. To change the information on the host database, it is necessary to delete the GLS configuration first, and configure it again after modifying the hostname information.
- As for configuring physical interface, be sure to define to use in TCP/IP before defining a virtual interface. (Check whether or not an /etc/hostname.interface file exists. If not, create it and reboot the system.)
- Set to activate a routing daemon because it is necessary to change the route information dynamically. If you are using Solaris 8 or Solaris 9 as a basic OS, you must not create the "/etc/defaultrouter" or "/etc/notrouter" file. Check whether the files exit, and if they do, change the file name or delete them. If you are using Solaris 10 for a basic OS, use the "routeadm(1M)" command to set up a routing daemon.

```
Routing daemon setup (Solaris 10 only):
# routeadm -e ipv4-forwarding
# routeadm -e ipv4-routing
# routeadm -s ipv4-routing-daemon="/usr/sbin/in.routed"
# routeadm -s ipv4-routing-daemon-args="-s"
# routeadm
                     Configuration   Current                 Current
                            Option   Configuration           System State
---------------------------------------------------------------
                IPv4 forwarding      enabled                 disabled
                   IPv4 routing      enabled                 disabled
                IPv6 forwarding      disabled                disabled
                   IPv6 routing      disabled                disabled

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

- For Redundant Line Control function, the path information must be initialized and the routing daemon must be restarted. If path information is statically specified, the static paths must be described in /etc/gateways.
- Because this mode uses dynamic routing by RIP, do not start RDISC (search protocol for ICMP router) during system startup. In order to restrain RDISC from starting, rename /usr/sbin/in.rdisc then reboot the system.

3.2.2.4 System setup in Fast switching/RIP mode

For the setup procedure, refer to “3.2.2.2 System setup in Fast switching mode” and “3.2.2.3 System setup in RIP mode”.

3.2.2.5 System setup in NIC switching mode

When using IPv4 address:

- When using an IPv4 address, define in the /etc/inet/hosts file the host names (host names to be attached to virtual IP, monitored host names to be specified in monitoring destination information, etc.) to be specified in environment definitions of Redundant

Line Control function. These host names must be specified in the /etc/inet/hosts file even if no host names but IP addresses are directly specified in environment definitions.

- When using an IPv4 address, define a configured primary physical interface to use in IPv4 before defining a virtual interface. (Check whether or not an /etc/hostname.interface file exists. If not, create it and reboot the system.)
- For Redundant Line Control function, the path information must be initialized and the routing daemon must be restarted. If path information is statically specified, the static paths must be described in /etc/gateways.

When using IPv6 address:

- If an IPv6 address is used, define the IPv6 address and a host name in /etc/inet/ipnodes file.
- When using an IPv6 address, define a configured physical interface to use in IPv6 before defining a virtual interface. (Check whether or not an /etc/hostname6.interface file exists. If not, create it and reboot the system. When creating a /etc/hostname6.interface file, make sure it is an empty file.)
- When using an IPv6 address, set an IPv6 router on a network to be connected without fail. Specify the same prefix and the same length of a prefix for an IPv6 address to be set in a Redundant Line Control function as those set in an IPv6 router.
  In addition, when you use a Solaris server as an IPv6 router, please define two or more server as an IPv6 router. When abnormalities occur in an IPv6 router, it becomes impossible to perform communication which used a site local address. Therefore, it recommends defining two or more IPv6 routers. When you define an IPv6 router as two or more servers, the prefix information on the virtual interface defined as /etc/inet/ndpd.conf should define the same value in each server.
  An example of setting a /etc/inet/ndpd.conf file when using a Solaris server as an IPv6 router is shown below. (See a Solaris manual for the detail of a /etc/inet/ndpd.conf file.)

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

3.2.2.6 System setup in GS/SURE linkage mode

- When using an IPv4 address, define in the /etc/inet/hosts file the host names (host names to be attached to virtual IP, monitored host names to be specified in monitoring destination information, etc.) to be specified in environment definitions of Redundant Line Control function. These host names must be specified in the /etc/inet/hosts file even if no host names but IP addresses are directly specified in environment definitions.
- The physical interface to be specified must not be defined for normal use in TCP/IP. (Check whether or not an /etc/hostname.interface file exists. If it does, rename the file or delete it, and execute "/usr/sbin/ifconfig <interface> unplumb" command.)
- GS/SURE linkage mode requires dynamic routings, so do not create /etc/defaultrouter file. (Check for existence of /etc/defaultrouter. If the file exists, either delete the file or rename the file.)
- It is necessary to block leaks of routing information from the system. If you are using Solaris 8 or Solaris 9 for a basic OS, create the "/etc/notrouter" file. If you are using Solaris 10 for a basic OS, use the "routeadm(1M)" command to set up a routing daemon.

```
Routing daemon setup (Solaris 10 only):
# routeadm -e ipv4-routing
# routeadm -s ipv4-routing-daemon="/usr/sbin/in.routed"
# routeadm -s ipv4-routing-daemon-args="-q"
# routeadm
                    Configuration   Current                 Current
                           Option   Configuration           System State
---------------------------------------------------------------
                  IPv4 forwarding   disabled                disabled
                     IPv4 routing   enabled                 disabled
                  IPv6 forwarding   disabled                disabled
                     IPv6 routing   disabled                disabled
```

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

- If path information is statically specified, the static paths must be described in /etc/gateways.
- Because this mode uses dynamic routing by RIP, do not start RDISC (search protocol for ICMP router) during system startup. In order to restrain RDISC from starting, rename /usr/sbin/in.rdisc then reboot the system.

3.2.3 syslog setup

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

[Setting file]

/etc/syslog.conf

[Settings]

When enabling message output

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

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

When disabling message output
Delete "*.info" information from the setting file.

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

[Setting notification]

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

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

In the following case, 234 becomes the process ID.

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

(2) SIGHUP transmission

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

```
# kill -HUP 234
```

[Others]

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

3.2.4 Zone setup for Solaris container

This section describes how to create a Solaris zone.

If you use a virtual interface of the redundant line control function in a Solaris zone, be sure to check that the environment setting of the redundant line control function is completed on the global zone and that the virtual interface is enabled. For information on how to set up the environment of the redundant line control function, see "3.3 Additional system setup".

(1) Create a zone

The following example shows how to create a zone. Note that the zone name is "zone0", the IP address is 192.168.10.100", and the interface name is "sha0".

```
# zonecfg -z zone0
zone0: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0    <- Specify a root path of the zone.
zonecfg:zone0> add net    <- Set up a network interface
zonecfg:zone0:net> set address=192.168.10.100/24
zonecfg:zone0:net> set physical=sha0    <- Specify a virtual interface for fast switching mode.
zonecfg:zone0:net> end
zonecfg:zone0> export    <- Check the setting.
create -b
set zonepath=/zones/zone0
set autoboot=false
add inherit-pkg-dir
set dir=/lib
end
add inherit-pkg-dir
set dir=/platform
end
add inherit-pkg-dir
set dir=/sbin
end
add inherit-pkg-dir
set dir=/usr
```

```
end
add net
set address=192.168.10.100/24
set physical=sha0
end
zonecfg:zone0> verify    <- Check integrity.
zonecfg:zone0> commit    <- Register a zone.
zonecfg:zone0> exit      <- Zone setting is completed.
# zoneadm list -vc       <- Check if the zone is properly registered.
   ID NAME             STATUS         PATH
    0 global           running        /
    - zone0            configured     /zones/zone0
```

When you set a network interface for fast switching mode, specify "shaX" for the virtual interface name. For NIC switching mode, specify a physical interface name of the primary server of the redundant physical interface (e.g. hmeX). Also, specify the IP address that is the same as that of the physical interface.

(2) Install the zone

You can install a zone using the following steps;

```
# zoneadm -z zone0 install
Preparing to install zone <zone0>.
Creating list of files to copy from the global zone.
Copying <3370> files to the zone.
Initializing zone product registry.
Determining zone package initialization order.
Preparing to initialize <1150> packages on the zone.
Initializing package <40> of <1150>: percent complete: 3%
. . . . . .
Initialized <1150> packages on zone.
Zone <zone0> is initialized.
Installation of <2> packages was skipped.
Installation of these packages generated warnings: <SUNWvtsr>
The file </zones/zone0/root/var/sadm/system/logs/install_log> contains a log of
the zone installation.
# zoneadm list -vc   <- Check if the zone is installed properly.
   ID NAME             STATUS         PATH
    0 global           running        /
    - zone0            installed      /zones/zone0
```

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

(3) Start the zone

Start the zone using the following steps. Before starting it, be sure to check the virtual interface is activated. If it is not activated, you cannot start the zone.

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

```
  sha0          Active      t     OFF    hme0(ON),hme1(ON)    <- Check the status.
[IPv6]
  Name          Status     Mode CL    Device
+----------+--------+----+----+-------------------------------------------------+
#
# zoneadm -z zone0 boot    <- Start the zone.
# zoneadm list –vc
   ID NAME                  STATUS             PATH
    0 global                running            /
    1 zone0                 running            /zones/zone0    <- Check if the zone is started properly.
```

(4) Log in to the zone

You can log in to the zone using the following steps:

```
# zlogin -l root zone0
[Connected to zone 'zone0' pts/4]
Sun Microsystems Inc.     SunOS 5.10          Generic January 2005
#
```

(5) Check the interface state

If you check the interface state on the zone, it will be displayed as follows:

```
# ifconfig -a
lo0:1: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232
index 1
        inet 127.0.0.1 netmask ff000000
sha0:1: flags=1000843<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu
1500 index 5
        inet 192.168.10.100 netmask ffffff00 broadcast 192.168.10.255
```

(6) Log out of the zone

You can log out of the zone using the following steps:

```
# exit

[Connection to zone 'zone0' pts/4 closed]
```

(7) Stop the zone

You can stop the zone using the following steps:

```
# zoneadm -z zone0 halt
# zoneadm list -vc
   ID NAME                  STATUS             PATH
    0 global                running            /
    - zone0                 installed          /zones/zone0
```

(8) Change the network setting

You can change the network setting using the following steps. In the following example, you are supposed to select the resource that is set "192.168.10.100" for the IP address, then change the interface name to "zone0", and the IP address to "192.168.20.123".

```
# zonecfg -z zone0
zonecfg:zone0> select net address=192.168.10.100   <- Select the resource.
zonecfg:zone0:net> set physical=hme0                <- Change the interface
zonecfg:zone0:net> set address=192.168.20.123       <- Change the IP address
zonecfg:zone0:net> end
zonecfg:zone0> export
create -b
set zonepath=/zones/zone0
set autoboot=false
add inherit-pkg-dir
set dir=/lib
end
add inherit-pkg-dir
set dir=/platform
end
add inherit-pkg-dir
set dir=/sbin
end
add inherit-pkg-dir
set dir=/usr
end
add net
set address=192.168.20.123   <- IP address changed
set physical=hme0            <- Interface name changed
end
zonecfg:zone0> verify
zonecfg:zone0> commit
zonecfg:zone0> exit
```

(9) Uninstall the zone

You can uninstall the zone using the following steps:

```
# zoneadm -z zone0 uninstall -F
# zoneadm list -vc
   ID NAME             STATUS         PATH
    0 global           running        /
    - zone0            configured     /zones/zone0
```

(10) Delete the zone

You can delete the zone using the following steps:

```
# zonecfg -z zone0 delete -F
# zoneadm list -vc
   ID NAME             STATUS         PATH
    0 global           running        /
```

For further details, see the "Solaris 10 OS" manual.

3.3 Additional system setup

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

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

3.3.1 Fast switching mode

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

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

When the Solaris zone is used

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

1. Create a virtual interface using "hanetconfig create" command.
2. After creating the configuration information, activate the concerned virtual interface using the "strhanet" command.
3. Create a zone. For information on how to create a zone, see "3.2.4 Zone setup for Solaris container".
4. Start the zone. The logical virtual interface (sha0:X) will be added to the virtual interface (sha0). The IP address specified during zone creation will be allocated.

3.3.2 RIP mode

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

1. Create a virtual interface using "hanetconfig create" command. If NICs are shared amongst several virtual interfaces, the same pair of physical interfaces should be specified to create each of the virtual interfaces with "hanetconfig create" command. For information, see Section "7.1 hanetconfig Command".
2. Setup the router/HUB monitoring function using the “hanetpoll create” command (only if the router/HUB monitoring function is used). For information, see Section "7.7 hanetpoll Command".

3.3.3 Fast switching/RIP mode

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

1. Create a virtual interface using "hanetconfig create" command. If NICs are shared amongst several virtual interfaces, the same pair of physical interfaces should be specified to create each of the virtual interfaces with "hanetconfig create" command. For information, see Section "7.1 hanetconfig Command".
2. Set up the router/HUB monitoring function using the “hanetpoll create” command (only if the router/HUB monitoring function is used). For information, see Section "7.7 hanetpoll Command".

3.3.4 NIC switching mode

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

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

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

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

When the Solaris zone is used

If you want to use a redundant physical interface of NIC switching in the Solaris zone, it is necessary to add the configuration as follows;

1. Set up a virtual interface using the "hanetconfig create" command.
2. Set up the standby patrol function using the "hanetconfig create" command (only if the standby patrol function is used). It is not necessary to set if a standby patrol function is already set in a virtual interface that already shares NIC.
3. Set up the router/HUB monitoring function using the "hanetpoll create" command.
4. Specify "plumb" to deactivate a standby interface using the "hanetparam -d" command.
5. After creating the configuration information, activate the concerned virtual interface using the "strhanet" command.
6. Start router/HUB monitoring function to monitor the routers/hubs using "hanetpoll on" command.
7. Create a zone. For information on how to create a zone, see "3.2.4 Zone setup for Solaris container".
8. Start the zone. The logical virtual interface (hme0:X) will be added to the primary interface (hme0) from the redundant physical interface (sha0). The IP address specified during zone creation will be allocated.

- In NIC switching mode, physical interfaces are activated or deactivated when switching over the transfer path. However, these changes are not recorded to a log file by default. For recording logs of these processes, refer to "3.2.3 syslog setup".
- In NIC switching mode with tagged VLAN interfaces, configure the standby patrol function on only one of virtual interfaces, if multiple virtual interfaces exist on the same pair of physical interfaces, and do not configure the standby patrol function on the other virtual interfaces. Note that, in general, the standby patrol function is not need to be configured on every single virtual interface.
- You cannot build an environment in which only one NIC is shared on multiplex physical interface on NIC switching mode using tagged VLAN interface.
- When configuring a standby patrol function for a virtual interface which is using the tagged VLAN interfaces, it is required to reboot the OS in order to enable the standby patrol function. GLS withholds a modification of MAC address of the secondary interface, so that it prevents communication errors on other tagged VLAN interfaces which are sharing a physical communication line.
- Ensure to specify the same IP address configured in /etc/hostname."interface-name" 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 "D.2.3.1 Switching takes place in NIC switching mode regardless of failure at the monitoring end".
- If you specify a physical interface of NIC switching for the network setting of the Solaris container (zone), it is necessary to change the method of deactivating a standby interface from "unplumb" to "plumb" using the "hanetparam -d" command. For details, see "7.6 hanetparam Command".

3.3.5 GS/SURE linkage mode

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

1. Set up a virtual interface using the “hanetconfig create” command. For information, see Section "7.1 hanetconfig Command".
2. Set up the remote party monitoring function using the “hanetobserv create” command. For information, see Section "7.5 hanetobserv Command".
   To change the monitoring period or number of monitoring times of this remote party, use “hanetpoll on” command. Refer to "7.7 hanetpoll Command" for details.

3.3.6 Setting parameter for individual mode

See the following procedure for using a value different from the default value indicated in section “3.1.2.6 Configuration of individual mode”.

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

3.4 Changing system setup

This section explains a procedure of modifying the system setup.

- The configuration command of a Redundant Line Control function can be executed only when the system is operating in multi-user mode.
- Once the setup is completed for Redundant Line Control function, the information regarding the host name (host name information over host database such as /etc/inet/hosts file) cannot be changed. To modify the information on host database, remove Redundant Line Control function configuration, and modify the information on the host database, then reconfigure the system.

- Once configuration is completed, “resethanet -s” command allows you to reflect the settings without rebooting the system. For details on this command refer to "7.15 resethanet Command".

3.4.1 Fast switching mode

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

1. Inactivate the concerned virtual interface using the “stphanet” command. For information, see Section "7.3 stphanet Command".
2. Change the configuration information.
3. After changing the configuration information, activate the concerned virtual interface using the “strhanet” command. For information, see Section "7.2 strhanet Command".

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

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

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

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

When the Solaris zone is used

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

1. Stop the Solaris zone.
2. Inactivate the concerned virtual interface using the "stphanet" command.
3. Change the configuration information.

4. Change the network settings. For information on how to change the zone network settings such as virtual IP address, see "3.2.4 Zone setup for Solaris container".
5. After changing the configuration information, activate the concerned virtual interface using the "strhanet" command.
6. Start the zone.

3.4.2 RIP mode

The following shows the procedure for changing configuration information for RIP mode:

1. Inactivate the concerned virtual interface using the “stphanet” command. For information, see Section "7.3 stphanet Command".
2. Stop the monitoring information (only if monitoring is enabled). For information, see Section "7.7 hanetpoll Command".
3. Change the configuration information.
4. After changing the configuration information, activate the concerned virtual interface using the “strhanet” command.
5. Start monitoring (only if monitoring is enabled). For information, see Section "7.7 hanetpoll Command".

The following lists the information that can be changed for RIP 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".
  - Operation mode (Only RIP mode or Fast switching/RIP mode can be selected.)
  - 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
- Data of monitored remote system and parameters
  Use the “hanetpoll” command to change the following information. For information, see Section "7.7 hanetpoll Command".
  - Monitored remote system data (primary monitored remote system IP address and secondary monitored remote system IP address)
  - Monitoring interval
  - The number of monitoring times
  - The number of retries prior to stopping monitoring the router
  - Recovery monitoring period
  - Cluster switching
  - Link up waiting time

3.4.3 Fast switching/RIP mode

For information on the procedure for configuration information for Fast switching/RIP mode and the information items that can be changed, see Sections "3.4.1 Fast switching mode" and "3.4.2 RIP mode".

3.4.4 NIC switching mode

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

1. Stop the router/HUB monitoring function using "hanetpoll off" command. See "7.7 hanetpoll Command" for the detail.
2. Deactivate a virtual interface to change using a “stphanet” command. See "7.3 stphanet Command" for the detail.
3. Change the setup information and parameter. (This can be done when executing "hanetpoll on" command for changing the monitoring period, the number of monitoring times, the recovery monitoring period, the waiting time for cluster switching and a link-up.)
   See "7.7 hanetpoll Command" for the detail.
4. Deactivate temporarily all virtual interfaces set in NIC switching mode using a “stphanet” command, then reactivate them using a “strhanet” command. See "7.2 strhanet Command" and "7.3 stphanet Command" for the detail.
5. Start Router/HUB monitoring function to monitor the routers/hubs using "hanetpoll on" command.
   (Changes made to the monitoring period, the number of monitoring times, the

monitoring recovery period, the waiting time for a cluster failover, and the waiting time for a link up are reflected when "hanetpoll on" command is executed.)
See "7.7 hanetpoll Command" for the detail.

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

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

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

- Configuration definition information
  Use the “hanetconfig” command to change the following information. For information, see Section "7.1 hanetconfig Command".
  - Host name or IP address to be attached to a virtual interface or a logical virtual interface
  - A physical interface name for the virtual interface
  - An IP address or host name of the physical interface
- Standby patrol information
  Use the “hanetconfig” command to change the following information. For information, see Section "7.1 hanetconfig Command".
  - Local MAC address to be allocated to a standby NIC
  - Interface names to be bundled by a virtual interface
- Information of monitored remote system and parameters
  Use the “hanetpoll” command to change the following information. For information, see Section "7.7 hanetpoll Command".
  - Information on monitored remote system (primary monitored remote system IP address and secondary monitored remote system IP address)
  - HUB-to-HUB monitoring
  - Monitoring interval
  - The number of monitoring times
  - Cluster switching
  - Link up waiting time
- Use the “hanetparam” command to change the following information. For information, see Section “7.6 hanetparam Command”.
  - Standby patrol monitoring interval
  - The number of constant standby monitoring prior to outputting message

When the Solaris zone is used

If you want to use a redundant physical interface of NIC switching in the Solaris zone, it is necessary to add the configuration as follows;

1. Stop the Solaris zone.
2. Stop the router/HUB monitoring function using "hanetpoll off" command.
3. Deactivate a virtual interface to change using a "stphanet" command.
4. Change the setup information and parameter. (This can be done when executing "hanetpoll on" command for changing the monitoring period, the number of monitoring times, the recovery monitoring period, the waiting time for cluster switching and a link-up.)
5. Change the network settings. For information on how to change the zone network settings such as virtual IP address, see "3.2.4 Zone setup for Solaris container".
6. Deactivate temporarily all virtual interfaces set in NIC switching mode using a "stphanet" command, then reactivate them using a "strhanet" command.
7. Start Router/HUB monitoring function to monitor the routers/hubs using "hanetpoll on" command.
8. (Changes made to the monitoring period, the number of monitoring times, the monitoring recovery period, the waiting time for a cluster failover, and the waiting time for a link up are reflected when "hanetpoll on" command is executed.)
9. Start the zone.

- Ensure to specify the same IP address configured in /etc/hostname."interface-name" 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.

3.4.5 GS/SURE linkage mode

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

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

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

- Configuration definition information
  Use the “hanetconfig” command to change the following information. For information, see Section "7.1 hanetconfig Command".
  - Host name or IP address to be attached to a virtual interface or a logical virtual interface
  - Host name or IP address to be attached to a physical interface
  - Interface names to be bundled by a virtual interface
- Parameters
  Use the “hanetpoll” command to change the following information. For information, see Section "7.7 hanetpoll Command".
  - Monitoring interval
  - The number of monitoring times
  - Recovery monitoring period
  - Cluster switching
  - Link up waiting period
- Remote node information
  Use the “hanetobserv” command to change the following information. For information, see Section "7.5 hanetobserv Command".
  - Remote node name
  - Virtual IP information (Virtual IP address, Remote physical IP address, Monitoring on/off, Send RIP from remote host on/off, Network information of relaying host)

3.4.6 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.

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

- Use the “resethanet” command to delete the entire configured values of the virtual interface for Redundant Line Control function. For details on “resethanet” command, refer to "7.15 resethanet Command".

3.5.1 Fast switching mode

The following shows the procedure for deleting configuration information:

1. Inactivate the concerned virtual interface using the “stphanet” command. For information, see Section "7.3 stphanet Command".
2. Delete the configuration information of the concerned virtual interface. For information, see Section "7.1 hanetconfig Command".
3. When IPv4 address is being used, the corresponding /etc/hostname.interface file is deleted and the host name further defined as the /etc/inet/hosts file is deleted.
   When IPv6 address is being used, the corresponding /etc/hostname6.interface file is deleted and the host name further defined as the /etc/inet/ipnodes file is deleted.
   Moreover, a router public-relations setup from the virtual interface defined as the /etc/inet/ndpd.conf file is deleted.
   In addition, a /etc/inet/ndpd.conf file is deleted when only a router public-relations setup from a virtual interface exists in a /etc/inet/ndpd.conf file.

When the Solaris zone is used

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

1. Stop the Solaris zone.
2. Inactivate the concerned virtual interface using the "stphanet" command.
3. Delete the configuration information of the concerned virtual interface.
4. When IPv4 address is being used, the corresponding /etc/hostname.interface file is deleted and the host name further defined as the /etc/inet/hosts file is deleted.
   When IPv6 address is being used, the corresponding /etc/hostname6.interface file is deleted and the host name further defined as the /etc/inet/ipnodes file is deleted.
   Moreover, a router public-relations setup from the virtual interface defined as the /etc/inet/ndpd.conf file is deleted.
   In addition, a /etc/inet/ndpd.conf file is deleted when only a router public-relations setup from a virtual interface exists in a /etc/inet/ndpd.conf file.
5. Delete the zone or change the zone network settings. For information on how to change the zone network settings or delete the zone, see "3.2.4 Zone setup for Solaris container".

3.5.2 RIP mode

The following shows the procedure for deleting configuration information:

1. Stop the router/HUB monitoring function using the “hanetpoll off” command (only if the router/HUB monitoring function is used). For information, see Section "7.7 hanetpoll Command".
2. Inactivate the concerned virtual interface using the “stphanet” command. For information, see Section "7.3 stphanet Command".
3. Delete the concerned monitoring destination information (only if the router/HUB monitoring function is used). For information, see Section "7.7 hanetpoll Command".
4. Delete the configuration information of the concerned virtual interface. For information,

see Section "7.1 hanetconfig Command".
5. Delete the /etc/hostname.interface file, and the host name defined as the /etc/inet/hosts file.

3.5.3 Fast switching/RIP mode

The following shows the procedure for deleting configuration information:

1. Stop the router/HUB monitoring function using the “hanetpoll off” command (only if the router/HUB monitoring function is used). For information, see Section "7.7 hanetpoll Command".
2. Inactivate the concerned virtual interface using the “stphanet” command. For information, see Section "7.3 stphanet Command".
3. Delete the concerned monitoring destination information (only if the router/HUB monitoring function is used). For information, see Section "7.7 hanetpoll Command".
4. Delete the configuration information of the concerned virtual interface. For information, see Section "7.1 hanetconfig Command".
5. Delete the /etc/hostname.interface file, and the host name defined as the /etc/inet/hosts file.

3.5.4 NIC switching mode

The following shows the procedure for deleting configuration information:

1. Use the “hanetpoll off” command with '-n' option to stop the HUB polling feature of the virtual interface targeted for deletion. This command, “hanetpoll off” with '-n' option allows you to stop the virtual interface by specifying them individually. For information, see Section "7.7 hanetpoll Command".
2. Inactivate the virtual interface of the concerned NIC switching mode using the “stphanet” command. To delete the operated definition in a cluster system, deactivate a virtual interface of the standby patrol using the “stpptl” command (only when using a standby patrol function). For information, see Section "7.3 stphanet Command" and Section “7.11 stpptl Command”.
3. Delete the concerned monitoring destination information. For information, see Section "7.7 hanetpoll Command".
4. Delete the configuration information of the concerned virtual interface. For information, see Section "7.1 hanetconfig Command".
5. When IPv4 address is being used, the corresponding /etc/hostname.interface file is deleted and the host name further defined as the /etc/inet/hosts file is deleted.
   When IPv6 address is being used, the corresponding /etc/hostname6.interface file is deleted and the host name further defined as the /etc/inet/ipnodes file is deleted.

When the Solaris zone is used

If you want to use a redundant physical interface of NIC switching in the Solaris zone, it is necessary to add the configuration as follows;

1. Stop the Solaris zone.
2. Use the "hanetpoll off" command with '-n' option to stop the HUB polling feature of the virtual interface targeted for deletion. This command, "hanetpoll off" with '-n' option allows you to stop the virtual interface by specifying them individually.
3. Inactivate the virtual interface of the concerned NIC switching mode using the "stphanet" command.
   If the logical IP address takeover function is set, disable a virtual interface of standby patrol using the "stpptl" command. (only for standby patrol)
4. If you cancel network high-reliability through NIC switching in all zones, return the method of deactivating a standby interface to "unplumb" using the "hanetparam -d" command. If you continue network high-reliability through NIC switching in the other zones, do not return the method of deactivating a standby interface to "unplumb".
5. Delete the concerned monitoring destination information.
6. Delete the configuration information of the concerned virtual interface.
7. When IPv4 address is being used, the corresponding /etc/hostname.interface file is deleted and the host name further defined as the /etc/inet/hosts file is deleted.
   When IPv6 address is being used, the corresponding /etc/hostname6.interface file is deleted and the host name further defined as the /etc/inet/ipnodes file is deleted.
8. Delete the zone or change the zone network settings. For information on how to change the zone network settings or delete the zone, see "3.2.4 Zone setup for Solaris container".

3.5.5 GS/SURE linkage mode

The following shows the procedure for deleting configuration information:

1. Inactivate the concerned virtual interface using the “stphanet” command. For information, see Section "7.3 stphanet Command".
2. Delete the monitoring destination information of the concerned communication parties. For information, see Section "7.5 hanetobserv Command".
3. Delete the configuration information of the concerned virtual interface. For information, see Section "7.1 hanetconfig Command".
4. Delete the host name defined as the /etc/inet/hosts file.
5. Reboot the system.

3.5.6 Note on deleting configuration information

The following shows a note on deleting configuration information.

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

3.6 Setting Option Function

3.6.1 Configuring multiple virtual interfaces

Use the “hanetconfig” command to set the multiple virtual interfaces setting function. For details about this command, see "7.1 hanetconfig Command".

3.6.2 Switching cluster when all the transfer paths fails

In Fast switching mode, execute “hanetparam” command to switch the cluster when failure occurs in the whole transfer path, See “7.6 hanetparam Command” for detail.

Additionally, if failure occurs in the whole transfer path in RIP, NIC switching, GS/SURE linkage modes, use the “hanetpoll” command to switch the cluster. See "7.7 hanetpoll Command" for detail.

3.6.3 Running multiple modes on a single virtual interface

Use the “hanetconfig” command to set the concurrent operation function with other modes, by using one virtual interface. For details about this command, see the execution examples in Section "7.1 hanetconfig Command".

3.6.4 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".

3.6.5 Multiple logical virtual interface definition

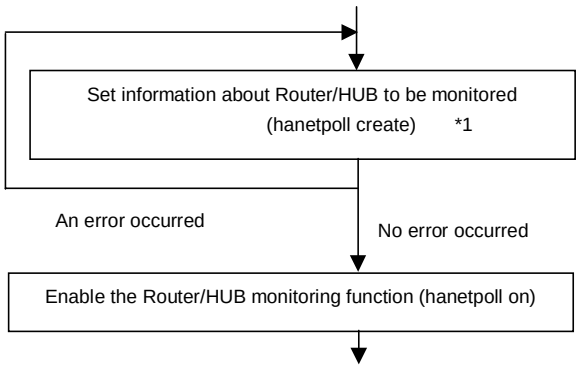
Use the “hanetconfig” command to set the multiple logical virtual interface definition function. For details about this command, see the execution examples in Section "7.1 hanetconfig Command".

3.6.6 Single physical interface definition

Use the “hanetconfig” command to set the single physical interface definition function. For details about this command, see the execution examples in Section "7.1 hanetconfig Command".

3.6.7 Router/HUB monitoring function

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



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

Figure 3.2 Setting procedure of the Router/HUB monitoring function

3.6.7.1 Creating monitoring information

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

3.6.7.2 Enabling Router/HUB monitoring function

Enable the Router/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 Router/HUB.

In NIC switching mode, no line failure is assumed even if the ping command fails until the link up wait time (IDLE (seconds) in Figure 3.3) passes. This is because monitoring starts after a physical interface is activated. Time required for link up depends on the HUB type to be connected. If the line monitoring fails although the HUB is not faulty, extend the wait time as required, using the -p parameter of the “hanetpoll on” command.

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

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

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

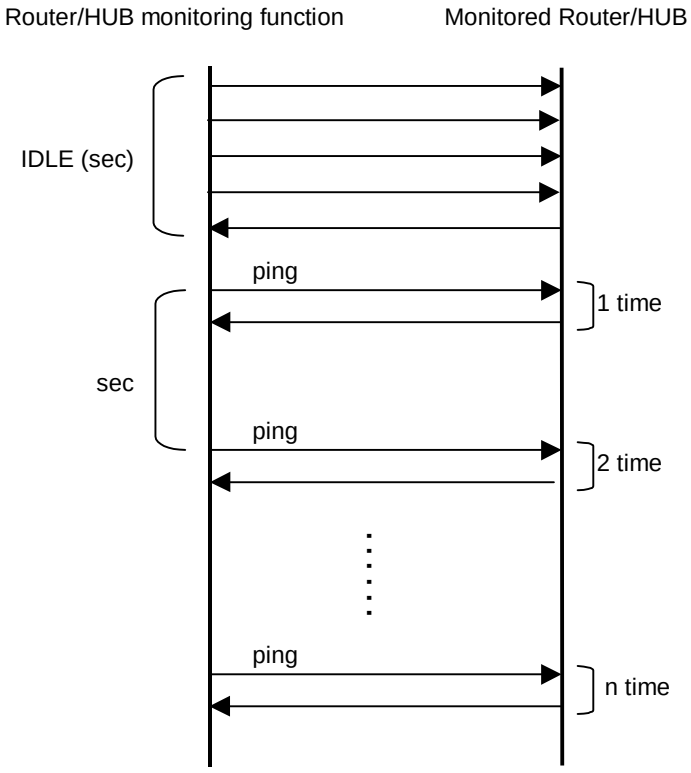


Figure 3.3 Basic sequence of Router/HUB monitoring

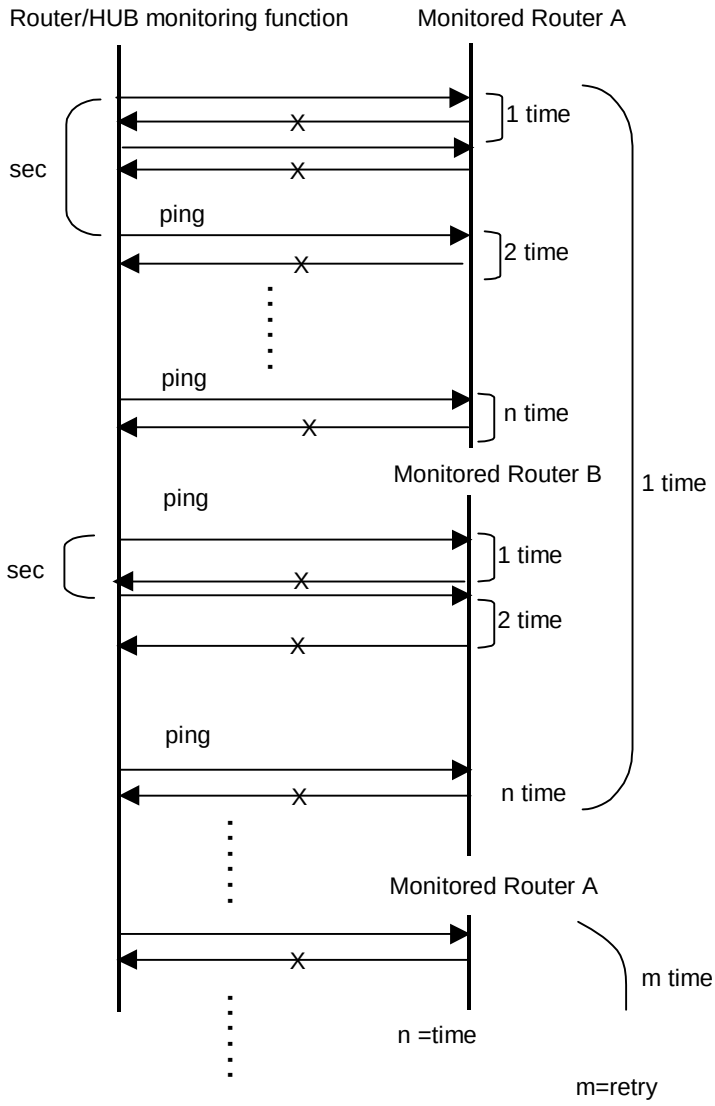


Figure 3.4 Router/HUB monitoring sequence after detect line fault

3.6.7.3 Transfer route error detection time for NIC switching mode

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

The followings are examples of the case of one monitoring target and two monitoring targets both using HUB-to-HUB monitoring feature.

One monitoring target:

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

*1: If the monitoring interval is 1 second, ping time out period would be 1 second, otherwise, ping time out period would be2 seconds.

The default value would look like the following.
5 sec x (5 – 1) + 2 sec = 22 sec

Two monitoring targets:

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

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

The default value would be like the following.
5 sec x (5 – 1) + 2 sec x 2 = 24 sec

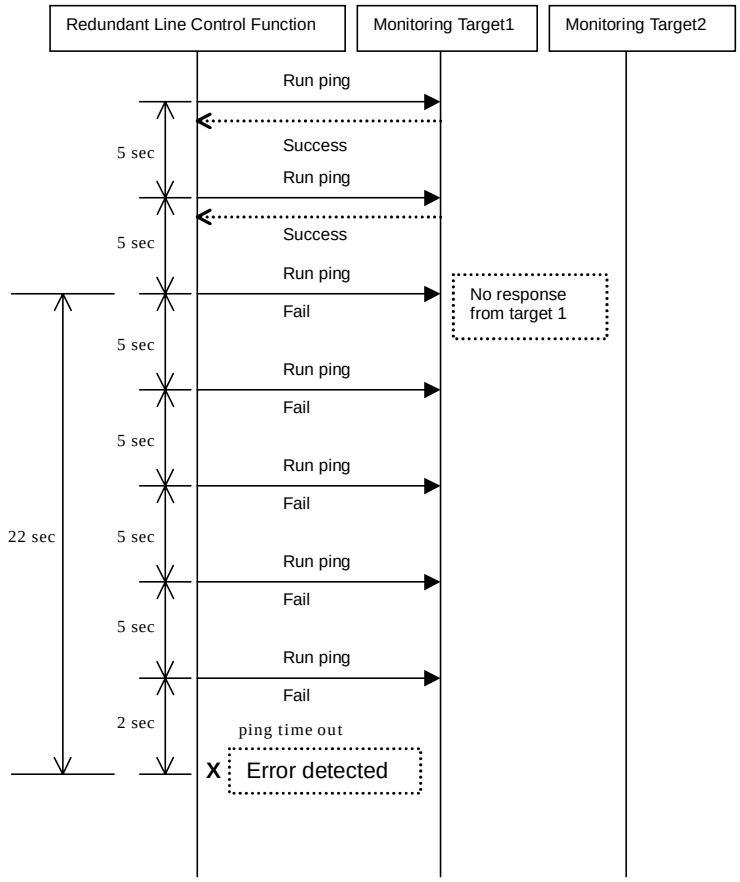


Figure 3.5 Transfer path error detection sequence (one monitoring target)

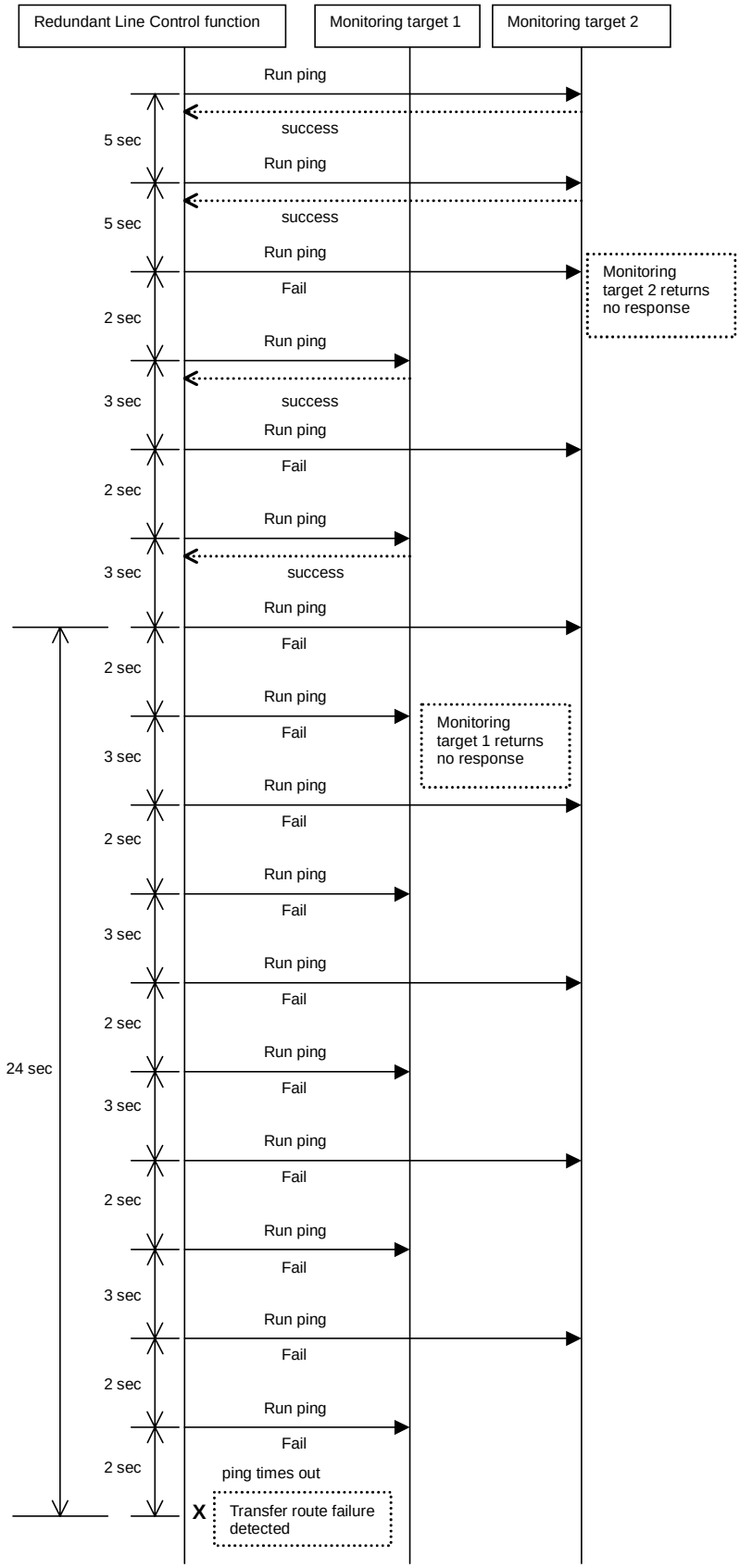


Figure 3.6 Transfer path error detection sequence (two monitoring target)

3.6.8 Monitoring the remote host

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

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

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

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

3.6.9 Standby patrol function

3.6.9.1 Setting what to be monitored

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

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

3.6.9.2 Setting monitoring interval

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

3.6.9.3 Setting error monitoring interval

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

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

3.6.10.1 Dynamic addition of physical interfaces

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

3.6.10.2 Dynamic deletion of physical interfaces

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

3.6.10.3 Dynamic switching of physical interfaces

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

3.6.11 Setting User command execution function

In NIC switching mode and GS/SURE linkage mode, a command pre-defined by a user can be executed at specific timing. For information on execution timing, see Section "2.2.12 User command execution function". In NIC switching mode, this function can be used to flush an ARP table, change the interface status, and change the MTU length, etc. In GS/SURE linkage mode, this function can be used to send a signal to a specific process, etc. The following settings must be made to execute a user command. See the sample files for information on creating a script file appropriate for a user's environment.

Sample file for NIC switching mode

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

Sample file for GS/SURE linkage mode

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

[Setup files]

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

Setup file for NIC switching mode

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

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

Setup file for GS/SURE linkage mode

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

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

- Do not call the operational command for redundancy line control function in the script file.
- The commands executed in the script file does not output message to the standard output. When checking for the contents of the outputted message, set the redirect path /dev/console/ and output the message to the console display. For detail, refer to the sample script file.
- 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.

3.6.11.1 Settings for NIC switching mode

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

(1) When activated or deactivated an IP address

[Script file call format]

/bin/sh shaX param1 param2 param3

param1
activate: Activated
inactivate: Inactivated

param2
before: Before activation or deactivation
after: After activation or deactivation

param3
ifname: Physical interface name

param4
inet6: Address family (IPv6 only)
* No param4 for IPv4.

[Definition file sample]

```
#!/bin/sh
#
#           All Rights Reserved, Copyright (c) FUJITSU LIMITED 2001
#
#ident    "%W% %G% %U% - FUJITSU"
#

#
#   Control interface for HA-Net
#

#
#           Params
#
#           $1          activate or inactivate
#           $2          before or after
#           $3          physical interface name
#           $4          address family (IPv6 only)
#

#
# Set Params
#

#INTERFACE=$3
#IP_ADDR1="xx.xx.xx.xx"
#IP_ADDR2="yy.yy.yy.yy"
#MAC_ADDR1="xx:xx:xx:xx:xx:xx"
#MAC_ADDR2="yy:yy:yy:yy:yy:yy"

cace $# in
3)
      ADDRESS_FAMILY="inet"
;;
4)
      if [ $4 = “inet6” ]
      then
            ADDRESS_FAMILY="inet6"
```

```
        else
                ADDRESS_FAMILY="unknown”
        fi
;;
*)
        ADDRESS_FAMILY="unknown”
;;
esac

if [ $ADDRESS_FAMILY = "inet" ]
then

case "$1" in
'activate')

#
# Activate interface
#

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

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

#if [ ! $INTERFACE = "hmeX" ]
#then
#       ifconfig $INTERFACE ether $MAC_ADDR1
#else
#       ifconfig $INTERFACE ether $MAC_ADDR2
#fi

;;

'after')
#
# script after activate interface
#

# echo "execute script after activate interface on" $INTERFACE > /dev/console

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

;;

*)
            ;;
esac

;;

'inactivate')
#
# inactivate interface
#
```

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

# 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
```

[Setting example]

The following shows an example of outputting a message when a command is executed, change the MTU length, deleting the concerned information from the ARP table, and checking the communication (executes the ping command).
Note that three-digit numbers placed on the left end of this example need not be placed in the actual script file because they just indicate line numbers for the purpose of explanation.

* An example of setting operated only in IPv4.

```
001 #!/bin/sh
002 #
003 #           All Rights Reserved, Copyright (c) FUJITSU LIMITED 2001
004 #
005 #ident    "%W% %G% %U% - FUJITSU"
006 #
007
008 #
009 #    Control interface for HA-Net
010 #
011
012 #
013 #           Params
014 #
015 #           $1          activate or inactivate
016 #           $2          before or after
017 #           $3          physical interface name
018 #
019
020 #
021 # Set Params
022 #
023
024 INTERFACE=$3
025 IP_ADDR1="192.1.1.1"
026 IP_ADDR2="192.1.2.1"
027 MAC_ADDR1="02:00:00:00:00:00"
028 MAC_ADDR2="02:00:00:00:00:01"
029
030 case "$1" in
031'activate')
032
033 #
034 #    Activate interface
035 #
036 case "$2" in
037 'before')
038 #
039 # script before activate interface
040 #
041
042 echo "execute script before activate interface on" $INTERFACE > /dev/console
043 if [ ! $INTERFACE = "hmeX" ]
044 then
045             ifconfig $INTERFACE ether $MAC_ADDR1
046 else
047             ifconfig $INTERFACE ether $MAC_ADDR2
048 fi
049 ;;
050
051 'after')
052 #
053 # script after activate interface
054 #
```

```
055 echo "execute script after activate interface on" $INTERFACE > /dev/console
056 ifconfig $INTERFACE mtu 1454
057 if [ ! $INTERFACE = "hmeX" ]
058 then
059             arp -d $IP_ADDR1
060             ping $IP_ADDR2 2
061 else
062             arp -d $IP_ADDR2
063             ping $IP_ADDR1 2
064 fi
065 ;;
066 *)
067             ;;
068 esac
069
070 ;;
071
072 'inactivate')
073 #
074 #    inactivate interface
075 #
076
077 case "$2" in
078 'before')
079 #
080 # script before inactivate interface
081 #
082
083    echo "execute script before inactivate interface on" $INTERFACE >
/dev/console
084 ;;
085
086 'after')
087 #
088 # script after inactivate interface
089 #
090
091    echo "execute script after inactivate interface on" $INTERFACE > /dev/console
092 ;;
093
094 *)
095               ;;
096 esac
097
098 ;;
099
100 *)
101               ;;
102 esac
103
104 exit 0
```

The following explains this setting example. In the explanation, [xxx] represents a line number in this setting example.

[031-071]: Describe the processing of activating the interface.

[042-050]: Outputs a message that a command is executed and sets the interface information (MAC address) depending on the interface type to be processed before the interface is activated.

[055-064]: Outputs a message for executing command. Then, changes the length of MTU after activating the interface. Finally, it deletes the corresponding ARP information and checks for a communication.

[072-099]: Describe the processing of inactivating the interface.

[083-084]: Outputs a message that a command is executed before the interface is inactivated.

[090-092]: Outputs a message that a command is executed after the interface is inactivated.

(2) When detected an error in a transfer route

[Script file call format]

/bin/sh shaX param1

param1
Primary: Error in a Primary interface
Secondary: Error in a Secondary interface
all: Error in both Primary/Secondary interfaces

[Definition file sample]

```
#!/bin/sh
#
#             All Rights Reserved, Copyright (c) FUJITSU LIMITED 2002
#
#ident    "%W% %G% %U% - FUJITSU"
#
# Control interface for HA-Net
#
#
#         Params
#
#         $1    communication line state        primary/secondary/all
#
#
# Set Params
#
#STATE=$1
#PROC="process_name"
#kill -15 `/usr/bin/ps -e | /usr/bin/sed -n ¥
#             -e'/'$PROC'$/s/[^0-9 ¥t].*//p' ¥
#             ` > /dev/null 2>/dev/null
#if [ $STATE = "primary" ]
#then
# echo "execute script Polling fail : primary" > /dev/console
#fi
#if [ $STATE = "secondary" ]
#then
# echo "execute script Polling fail : secondary" > /dev/console
#fi
#if [ $STATE = "all" ]
#then
# echo "execute script Polling failover" > /dev/console
#fi
```

(3) When detected a standby patrol error or recovery

[Script file call format]

/bin/sh shaX param1 param2

param1
establish: Standby patrol established
recover: Standby NIC monitoring recovered
fail: Standby NIC error

param2
Physical interface name of standby NIC: Physical interface name such as hmeX
unknown: Standby NIC undecided

[Definition file sample]

```
#!/bin/sh
#
#           All Rights Reserved, Copyright (c) FUJITSU LIMITED 2002
#
#ident    "%W% %G% %U% - FUJITSU"
#
# Control interface for HA-Net
#
#
#        Params
#
#        $1   standby NIC state     establish/recovery/fail
#        $2   standby NIC name       hmeX
#
#
# Set Params
#
#STATE=$1
#NIC=$2
#if [ $STATE = "fail" ]
#then
# echo "execute script Patrol fail ($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
```

3.6.11.2 Settings for GS/SURE linkage mode

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

[Script file call format]

/bin/sh hostIP

[Definition file sample]

```
#
#            All Rights Reserved, Copyright (c) FUJITSU LIMITED 2001
#
#ident    "%W% %G% %U% - FUJITSU"
#

#
#    Control interface for HA-Net
#

#
# Set Params
#

#PROC="process_name"

#
# Procedure
#

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

[Setting example]

The following shows an example of sending a signal (SIGHUP) to the DUMY process. Note that three-digit numbers placed on the left end of this example need not be placed in the actual script file because they just indicate line numbers for the purpose of explanation.

```
001 #
002 #            All Rights Reserved, Copyright (c) FUJITSU LIMITED 2001
003 #
004 #ident    "%W% %G% %U% - FUJITSU"
005 #
006
007 #
008 #    Control interface for HA-Net
009 #
010
011 #
012 # Set Params
013 #
014
015 PROC="DUMY"
016
017 #
018 # Procedure
019 #
020
020 #
030 kill -1 `/usr/bin/ps -e | /usr/bin/sed -n ¥
          -e'/'$PROC'$/s/[^0-9 ¥t].*//p' ¥
          ` > /dev/null 2>/dev/null
```

The following explains this setting example. In the explanation, [xxx] represents a line number in this setting example.

[015]: Specifies a process name to be stopped.

[030]: Acquires the process ID of a concerned process from the process list and send SIGTERM for the process.

3.7 Configuring other functions

3.7.1 Outputting message when transfer paths fails

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

3.7.2 Setting Dynamic Reconfiguration (DR)

This section explains the procedure of configuring Dynamic Reconfiguration (DR) of PRIMEPOWER 800/900/1000/1500/2000/2500 and GP7000F model 1000/2000.

3.7.2.1 Configure environment

When building LAN environment for redundancy system using Redundant Line Control function, in order to replace or add the hardware without stopping the communication using Dynamic Reconfiguration, it is recommended to build the environment shown in figure 3.7 “Recommended LAN configuration”.

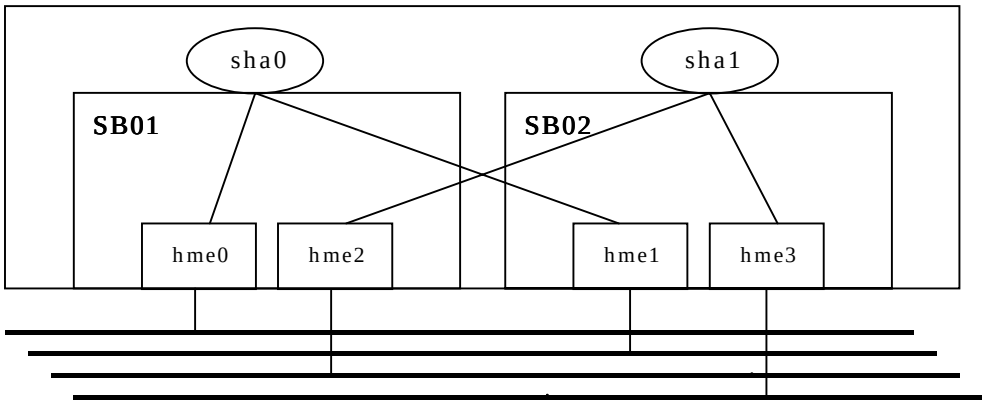


Figure 3.7 Recommended LAN configuration

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

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

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

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

3.7.3 Transfer route multiplexing with Tagged VLAN interface

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

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

3.7.3.1 Operating VLAN interface on Fast switching mode

When bundling a tagged VLAN interface on Fast switching mode, specify the tagged VLAN interface instead of the physical interface. The Figure 3.8 illustrates bundled tagged VLAN architecture.

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

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

Figure 3.8 illustrates an example of using tagged VLAN interface on Fast switching mode.

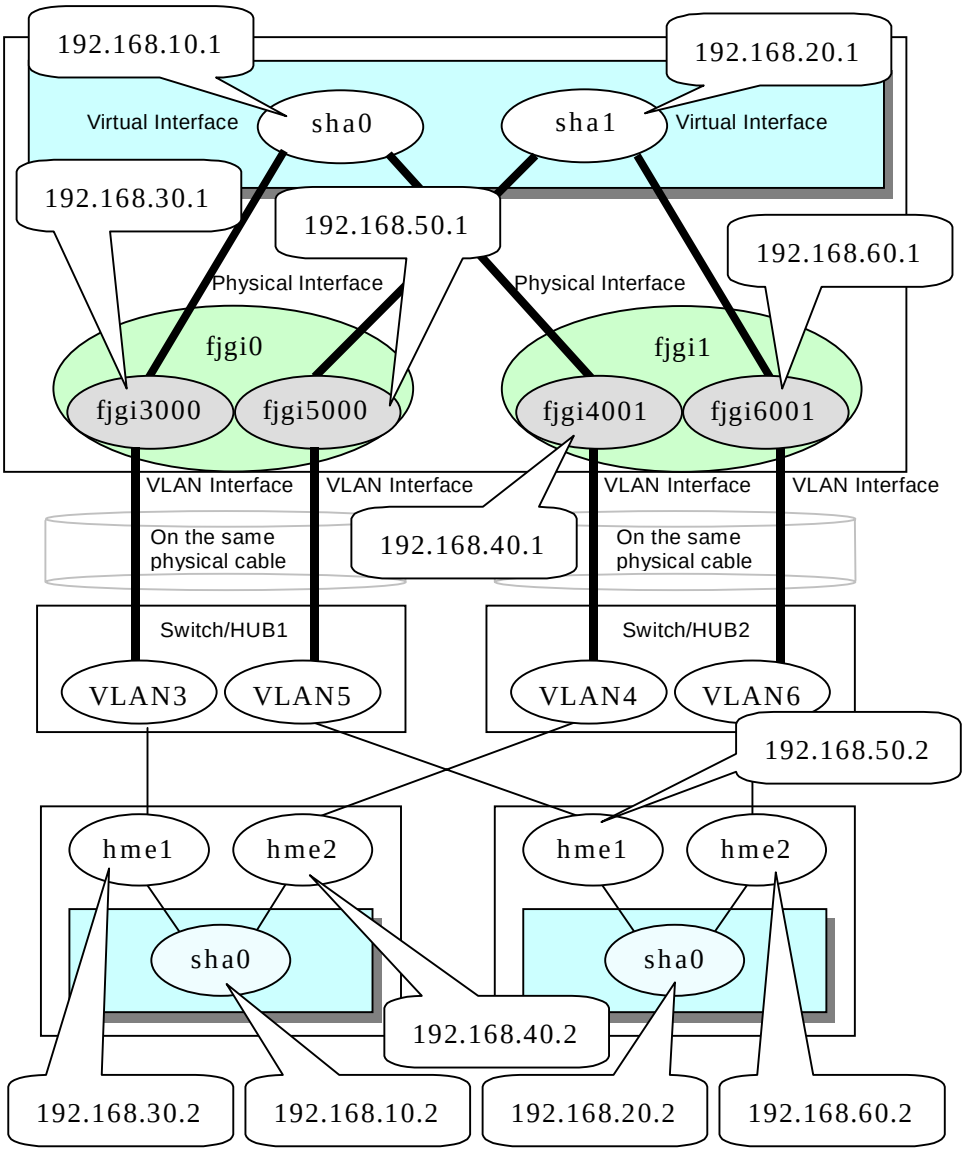


Figure 3.8 Fast switching mode with tagged VLAN interface

3.7.3.2 Operating VLAN interface on NIC switching mode

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

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

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

Synchronized switching of virtual interfaces

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

interface is chosen.

Figure 3.9 illustrates of synchronous switching architecture.

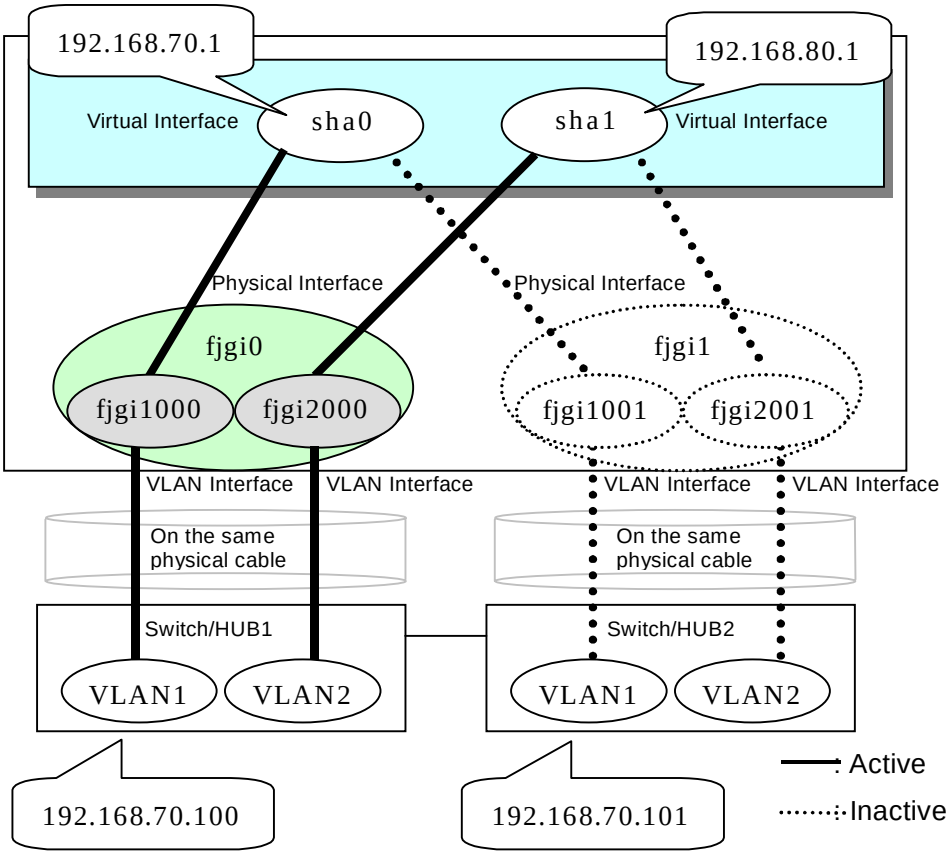


Figure 3.9 NIC switching mode with tagged VLAN interface (synchronized switching)

Asynchronous switching of virtual interfaces

Contrary to a synchronous switching, two or more virtual interfaces which bundle multiple tagged VLAN interfaces, can be switched asynchronously. In this case, the monitoring target IP address from which it differs for every virtual interface is defined as monitoring target information.
When two or more definitions of the IP address for management are possible to switch/HUB used as a monitoring target, the asynchronous switching of the virtual interfaces is chosen to use Standby NIC effectively.

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

Figure 3.10 illustrates of asynchronous switching architecture.

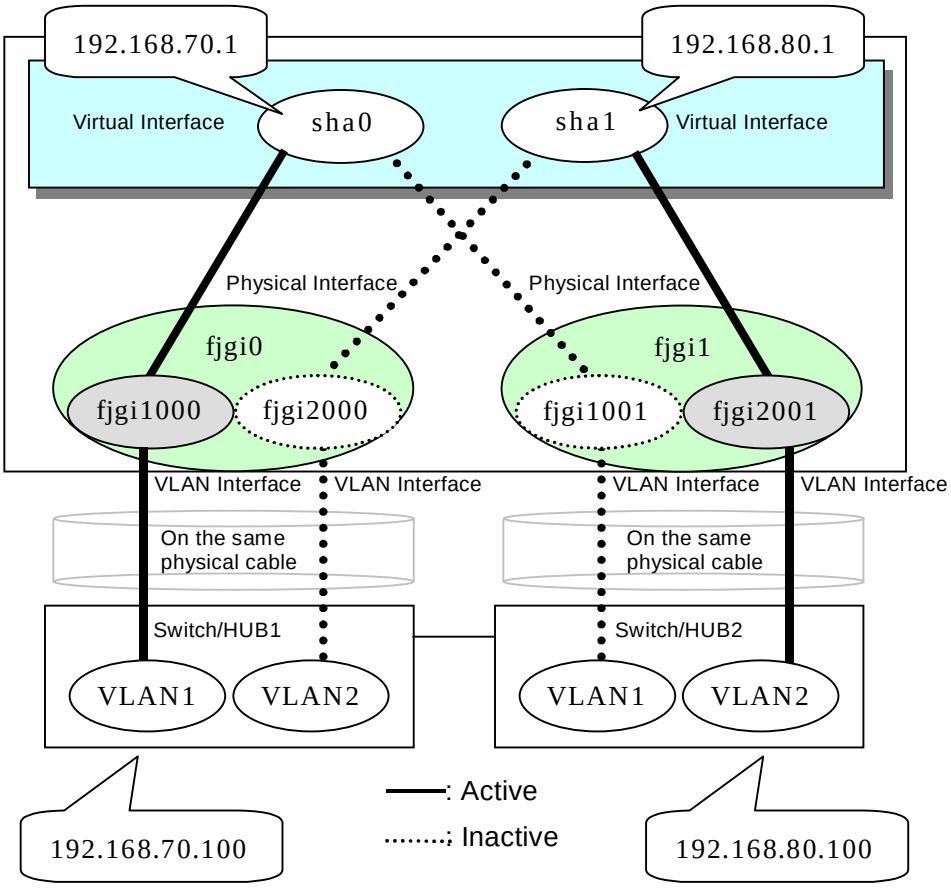


Figure 3.10 NIC switching mode with tagged VLAN interface (asynchronous switching)

Note

- On NIC switching mode, if several tagged VLAN interfaces exist on two physical interfaces, and at lease two virtual interfaces are created on pairs of those tagged VLAN interfaces, please ensure that you configure the standby patrol function exclusively on a single virtual interface. For example, say virtual interface (sha0) is created on two tagged VLAN interfaces "fjgi1000" and "fjgi1001", and similarly, another virtual interface (sha1) is created on "fjgi2001" and "fjgi2000", the standby patrol function must be configured on either one of the virtual interfaces (sha0 or sha1).
- On NIC switching mode, tagged VLAN interfaces on a pair of physical interfaces should be used to create multiple virtual interfaces, if tagged VLAN networks are used. For example, you cannot have an environment where a virtual interface is created on a pair of VLAN interfaces "fjgi1000" and "fjgi1001", and another virtual interface is created on a pair of VLAN interfaces "fjgi2001" and "fjgi2002" because the physical interface "fjgi1" is the only shared physical interface here.
- When using synchronized switching mode with tagged VLAN interfaces, only one virtual interface is selected to switch/HUB monitoring. Its interface address is the nearest to monitoring target.
- If you specify two monitoring targets with synchronized switching mode, please specify two network addresses which belong to the same network. If their network addresses are different, switch/HUB monitoring cannot operate normally, because they are assigned to only one virtual interface.
- When configuring a standby patrol function for a virtual interface which is using the tagged VLAN interfaces, it is required to reboot the OS in order to enable the standby patrol function. GLS withholds a modification of MAC address of the secondary interface, so that it prevents communication errors on other tagged VLAN interfaces which are sharing a physical communication line.

- When the physical IP address takeover function of the NIC switching mode is used, a virtual interface cannot be synchronized switched.

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 below lists the Redundant Line Control function operation commands.

Table 4.1 Redundant Line Control function operation commands

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

4.1 Starting and Stopping Redundant Line Control function

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

4.1.1 Starting Redundant Line Control function

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

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

4.1.2 Stopping Redundant Line Control function

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

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

4.2 Activating and Inactivating Virtual Interfaces

This section explains how to activate and inactivate virtual interfaces.

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

4.2.1 Activating virtual interfaces

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

For details about this command, see Section "7.2 strhanet Command".

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

4.2.2 Inactivating virtual interfaces

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

For details about this command, see Section "7.3 stphanet Command".

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

4.3 Displaying Operation Status

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

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

4.4 Displaying Monitoring Status

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

For information on this command, see Section "7.8 dsppoll Command".

4.5 Dynamic operation (Replacement / Expansion)

In Redundant Line Control function, it is possible to replace or add redundant NIC (PCI card) by linking with Dynamic Reconfiguration (DR) and PCI Hot Plug (PHP). (Keep in mind that Fast Switching mode and NIC Switching mode with defined IPv6 in the virtual interface cannot replace or add NICs)

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

Dynamic operation	**Compatible system**
DR(Dynamic Reconfiguration)	PRIMEPOWER 800/900/1000/1500/2000/2500 and GP7000F model 1000/2000
PHP(PCI Hot Plug)	PRIMEPOWER 450/900/1500/2500/HPC2500

4.5.1 Executing DR command

(1) Disconnecting a system board

When cut off using a DR command (drc -disconnect), an actual interface on the corresponding system board is automatically cut off from a virtual interface according to a DR connection script of a Redundant Line Control function.
It is not possible to disconnect a system board if a virtual interface (sha0 etc) and a physical interface have been configured on it. A DR connection script outputs a message and ends abnormally.
In this case, deactivate a virtual interface configured by a physical interface on a system board to be cut off, and execute a DR command (drc -disconnect) after deleted a definition.

(2) Connecting a system board

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

(3) Cancellation

In case the system wants to stop executing DR process due to a certain reason, or if the user requests to stop it while a DR command is executed, the system cancels execution of the DR command.
Through the DR connection script of GLS, the disconnection process can be stopped, and the environment is restored to the original state.

[Notes]

- While exchanging a system board containing a physical interface that has been used to configure a virtual interface in NIC switching mode, HUB monitoring function halts temporarily since it is not possible to switch NICs even if an error occurs in a transfer route.
- After replacing a system board containing a physical interface used to configure a virtual interface in NIC switching mode, monitoring of a transfer route will start normally.

4.5.2 Replacement/Expansion PHP (PCI Hot Plug)

This section explains a procedure of replacing or adding a PCI card for GLS in a PCI Hot Plug (PHP) environment.

PCI Hot Plug (PCI Hot Plug) is supported by PRIMEPOWER 450/900/1500/2500/HPC2500.

Compatibility of PHP with each mode is shown in the table below.

[PHP Support] A: Supported X: Not supported

PHP(PCI Hot Plug) operation	Fast switching mode	RIP mode	NIC switching mode	GS/SURE linkage mode
Replacement (Redundant system)	A	X	A	A
Extension (Non-redundant system)	A	X	A	A
Extension (Redundant system)	A	X	X	A

Replacement and expansion of PHP (PCI Hot Plug) is allowed only when the system is running in a multiple user mode.

4.5.2.1 Replacement of PCI card on redundant system

In Fast Switching and NIC Switching mode, it is possible to replace the redundant NIC without stopping network communication.

For NIC Switching mode, it is required to stop the transfer path monitoring function and standby patrol function.
For GS/SURE linkage mode, it is required to deactivate the virtual interface.

The following is a procedure of replacing redundant system.

For replacing procedure of deactivated configuration, refer to “PCI Hot Plug User’s guide for I/O device”.

1) Stop the hardware monitoring of the Machine Administration

The hardware monitoring of the Machine Administration is stopped by using the following command.

```
# /usr/sbin/FJSVmadm/prephp <Return>
```

2) Specify the replacing PCI card

An interface on the PCI card to be replaced can be identified from the warning messages output to the console (eg. hme1).

3) Disconnect from redundant system

In order to remove the PCI card from the redundant system for replacement, please execute the following command with the interface name obtained in the procedure "2) Specify the replacing PCI card". On the redundant system of standby mode, when an online communication path is disconnected, a standby communication path will be online communication path automatically.

Fast switching mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i hme1 <Return>
# /usr/sbin/ifconfig hme1 unplumb <Return>
```

NIC switching mode

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off <Return>
# /opt/FJSVhanet/usr/sbin/stpptl -n sha1 <Return>
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
```

GS/SURE linkage mode

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

4) Disconnect the PCI card

Specify the interface name identified in the procedure "2) Specify the replacing PCI card." to "inst2comp" command to obtain the PCI bus slot "Ap_Id".

```
# /usr/sbin/FJSVmadm/inst2comp hme1 <Return>
pcipsy21:R0B01-PCI#slot03
```

Specify the "Ap_Id" obtained above as an argument to "cfgadm"(1M) command, and confirm that the slot status of the PCI card to be disconnected is "connected configured".

```
# cfgadm pcipsy21:R0B01-PCI#slot03 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy21:R0B01-PCI#slot03      pci-pci/hp   connected     configured    ok
```

Please disconnect the PCI card by executing the cfgadn (1M) command with "Ap_Id," and confirm that the slot status is "disconnected unconfigured."

```
# cfgadm -c disconnect pcipsy21:R0B01-PCI#slot03 <Return>
# cfgadm pcipsy21:R0B01-PCI#slot03 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy21:R0B01-PCI#slot03      unknown      disconnected  unconfigured  unknown
```

To indicate the slot position for replacement, specify the obtained "Ap_Id" to "cfgadm" command and blink the ALARM LED.

```
# cfgadm -x led=fault,mode=blink pcipsy21:R0B01-PCI#slot03 <Return>
```

5) Replace the PCI card

The PCI card disconnected in the procedure "4) Disconnect the PCI card" is replaced with a new one. Our customer support staff does this for you.

6) Connect the PCI card

In order to connect a new PCI card, execute "cfgadm" command with "configure" option and the "Ap_Id", or push the push button of the PCI bus slot.

In addition, a push button is valid only in multiple user mode.

Please confirm that the slot status is "connected configured" by using the cfgadm (1M) command after the above-mentioned procedure.

```
# cfgadm -c configure pcipsy21:R0B01-PCI#slot03 <Return>
# cfgadm pcipsy21:R0B01-PCI#slot03 <Return>
Ap_Id                          Type         Receptacle      Occupant
Condition
pcipsy21:R0B01-PCI#slot03      pci-pci/hp   connected       configured      ok
```

7) Connect to redundant system

In order to connect the new PCI card to a redundant system, please execute the following commands with the interface name identified in the procedure "2) Specify the replacing PCI card".

Fast switching mode

```
# /usr/sbin/ifconfig hme1 plumb <Return>
# /usr/sbin/ifconfig hme1 192.168.10.10 netmask + broadcast + -trailers up <Return>
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i hme1 <Return>
```

NIC switching mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
# /opt/FJSVhanet/usr/sbin/strptl -n sha1 <Return>
# /opt/FJSVhanet/usr/sbin/hanetpoll on <Return>
```

GS/SURE linkage mode

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

8) Switch back the redundant path

Please switch back an online communication path if needed.

9) Start the hardware monitoring of the Machine Administration

Please execute the following commands in order to update configuration information, and restart the hardware monitoring of the Machine Administration.

```
# /usr/sbin/FJSVmadm/postphp <Return>
```

4.5.2.2 Extension of PCI cards with new redundant system

By adding a new PCI card to a non-redundant system, it is possible to create a redundant system.

The following is the procedure of adding a new PCI card to a non-redundant system.

1) Stop the hardware monitoring of the Machine Administration

The hardware monitoring of the Machine Administration is stopped by using the following command.

```
# /usr/sbin/FJSVmadm/prephp <Return>
```

2) Add PCI cards

a.
Before adding a PCI card, please save the output of "prtpicl"(1M) command.

```
# prtpicl -v > /tmp/prtpicl.pre <Return>
```

b.
Check the status of the slot.
An example of adding a PCI card to a slot "R0B01-PCI#slot02" is shown in this section. "R0" in "R0B01-PCI#slot02" indicates the I/O cabinet number: 0, "B01" the PCI/Disk Box number: 1, and "slot02" the physical slot number: 02.
If you are adding more PCI cards, please repeat the procedures 2) b and 3).
The relationship of the position of a PCI card and format of "Ap_Id" is shown below. (N: an integral number)

Location of PCI slot	**Element**	**Format of "Ap_Id"**
Cabinet of PRIMEPOWER 900/1500/2500	Cabinet Number: **X** System Board Number: **Y** Physical Slot Number: **ZZ**	pcipsyN:C**X**M0**Y**-PCI#slot**ZZ**
PCI / Disk BOX	I/O Cabinet Number: **X** PCI/Disk BOX Number: **Y** Physical Slot Number: **ZZ**	pcipsyN:R**X**B0**Y**-PCI#slot**ZZ**
other than those above	Physical Slot Number: **ZZ**	pcipsyN:PCI#slot**ZZ**

Please confirm that the status of the PCI slot where a PCI card is added is "empty unconfigured" by using "cfgadm" (1M) command.

```
# cfgadm R0B01-PCI#slot02 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy18:R0B01-PCI#slot02      unknown      empty         unconfigured  unknown
```

c.
To indicate the slot position for expansion, specify the "Ap_Id" identified in the procedure 2)b to "cfgadm" command and blink the ALARM LED.

```
# cfgadm -x led=fault,mode=blink pcipsy18:R0B01-PCI#slot02 <Return>
```

d.
Add a PCI card after the READY LED of the target PCI bus slot has turned off.
This operation is performed by our customer support.

e.
Please confirm that the PCI slot status which extended PCI cards is "disconnected unconfigured" by using cfgadm (1M) command.

```
# cfgadm pcipsy18:R0B01-PCI#slot02 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy18:R0B01-PCI#slot02      unknown      disconnected  unconfigured  unknown
```

3) Connect PCI cards

An added PCI card is connected to the system by executing "cfgadm" command with "configure" option and "Ap_Id", or by pushing the push button of the PCI bus slot.

In addition, a push button is valid only in multiple user mode.

Please confirm that the slot status is "connected configured" by using the cfgadm (1M) command after the above-mentioned procedure.

```
# cfgadm -c configure pcipsy18:R0B01-PCI#slot02 <Return>
# cfgadm pcipsy18:R0B01-PCI#slot02 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy18:R0B01-PCI#slot02      pci-pci/hp   connected     configured    ok
```

4) Start the hardware monitoring of the Machine Administration

Please execute the following command in order to update configuration information, and restart the hardware monitoring of the Machine Administration.

```
# /usr/sbin/FJSVmadm/postphp <Return>
```

5) Connect equipment to PCI cards

The extended PCI card is connected with network equipment by the cable.

6) Setup driver

The driver configuration is added by following operations.

a.
The interface name is investigated in order to configure drivers and high layer products.
Please save the result of the prtcicl (1M) command, and obtain the difference information between current result and the result taken at "2.a." Then, the driver instance number for the extended PCI card is obtained.
In the following example, since the instance number is 1, it can be determined that the interface name of the extended PCI card is "hme1."

```
# prtpicl -v > /tmp/prtpicl.post <Return>
# diff /tmp/prtpicl.pre /tmp/prtpicl.post | more <Return>
                :
>       :status       okay
>       :devfs-path       /pci@8d,2000/network@1
>       :driver-name      hme
>       :binding-name     SUNW,hme
>       :bus-addr     1
>       :instance     1
>       :_class       obp-device
>       :name     network
                :
```

b.
Confirm that the interface name that is obtained from the above operation matches the one that has been added to the PCI bus slot.

```
# /usr/sbin/FJSVmadm/inst2comp hme1 <Return>
pcipsy18:R0B01-PCI#slot02
```

c.
The configuration of each driver is added.
Please refer to each driver manual for details.

7) Setup redundant system

Activate the virtual interface after configuring Fast Switching, NIC Switching, or GS/SURE linkage mode. System reboot is not required after configuring each mode.

When configuring Fast Switching mode, the added interface “hme1” must be activated preliminary by the following command.

For IPv4 address

```
# /usr/sbin/ifconfig hme1 plumb <Return>
# /usr/sbin/ifconfig hme1 IP address netmask + broadcast + -trailers up <Return>
```

For IPv6 address

```
# /usr/sbin/ifconfig lo0 inet6 plumb up <Return>
# /usr/sbin/ifconfig hme1 inet6 plumb up <Return>
```

For IPv4, the IP address specified in this section must also be defined in /etc/inet/hosts and /etc/hostname.hme1.
For IPv6, create /etc/hostname6.hme1 as an empty file.
Unless these are configured, when the system reboots, the virtual interface for Fast Switching mode cannot be activated.

4.5.2.3 Extension of PCI cards to redundant system

It is possible to extend a PCI card to the redundant system.

In NIC Switching mode, it is not possible to add a new interface to a redundant system.
Also, when adding a new interface in GS/SURE linkage mode, it is first required to deactivate the virtual interface for GS/SURE linkage mode and then add a new interface.

The following is the procedure of extending PCI card to the redundant system.

1) Stop the hardware monitoring of the Machine Administration

The hardware monitoring of the Machine Administration is stopped by using the following command.

```
# /usr/sbin/FJSVmadm/prephp <Return>
```

2) Add PCI cards

a.
Before extending the PCI card, please save the result (current configuration information) of the prtpicl (1M) command.

```
# prtpicl -v > /tmp/prtpicl.pre <Return>
```

b.
Check the status of the slot.
An example of adding a PCI card to a slot "R0B01-PCI#slot02" is shown in this section. "R0" in "R0B01-PCI#slot02" indicates the I/O cabinet number: 0, "B01" the PCI/Disk Box number: 1, and "slot02" the physical slot number: 02.
If you are adding more PCI cards, please repeat the procedures 2) b and 3).
The relationship of the position of a PCI card and format of "Ap_Id" is shown below. (N: an integral number)

Location of PCI slot	**Element**	**Format of "Ap_Id"**
Cabinet of PRIMEPOWER 900/1500/2500	Cabinet Number: **X** System Board Number: **Y** Physical Slot Number: **ZZ**	pcipsyN:C**X**M0**Y**-PCI#slot**ZZ**
PCI / Disk BOX	I/O Cabinet Number: **X** PCI/Disk BOX Number: **Y** Physical Slot Number: **ZZ**	pcipsyN:R**X**B0**Y**-PCI#slot**ZZ**
other than those above	Physical Slot Number: **ZZ**	pcipsyN:PCI#slot**ZZ**

Please confirm that the status of the PCI slot where a PCI card is added is "empty unconfigured" by using "cfgadm" (1M) command.

```
# cfgadm R0B01-PCI#slot02 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy18:R0B01-PCI#slot02      unknown      empty         unconfigured  unknown
```

c.
To indicate the slot position for expansion, specify the "Ap_Id" identified in the procedure 2)b to "cfgadm" command and blink the ALARM LED.

```
# cfgadm -x led=fault,mode=blink pcipsy18:R0B01-PCI#slot02 <Return>
```

d.
Add a PCI card after the READY LED of the target PCI bus slot has turned off. This operation is performed by our customer support.

e.
Please confirm that the PCI slot status which extended PCI cards is "disconnected unconfigured" by using cfgadm (1M) command.

```
# cfgadm pcipsy18:R0B01-PCI#slot02 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy18:R0B01-PCI#slot02      unknown      disconnected  unconfigured  unknown
```

3) Connect PCI cards

An added PCI card is connected to the system by executing "cfgadm" command with "configure" option and "Ap_Id", or by pushing the push button of the PCI bus slot.

In addition, a push button is valid only in multiple user mode.

Please confirm that the slot status is "connected configured" by using the cfgadm (1M) command after the above-mentioned procedure.

```
# cfgadm -c configure pcipsy18:R0B01-PCI#slot02 <Return>
# cfgadm pcipsy18:R0B01-PCI#slot02 <Return>
Ap_Id                          Type         Receptacle    Occupant
Condition
pcipsy18:R0B01-PCI#slot02      pci-pci/hp   connected     configured    ok
```

4) Connect equipment to PCI cards

The extended PCI card is connected with network equipment by the cable.

5) Setup driver

The driver configuration is added by following operations.

a.
The interface name is investigated in order to configure drivers and high layer products.
Please save the result of the prtcicl (1M) command, and obtain the difference information between current result and the result taken at "2.a." Then, the driver instance number for the extended PCI card is obtained.
In the following example, since the instance number is 1, it can be determined that the interface name of the extended PCI card is "hme2."

```
# prtpicl -v > /tmp/prtpicl.post <Return>
# diff /tmp/prtpicl.pre /tmp/prtpicl.post | more <Return>
                :
>       :status       okay
>       :devfs-path       /pci@8d,2000/network@2
>       :driver-name      hme
>       :binding-name     SUNW,hme
>       :bus-addr     2
>       :instance     2
>       :_class       obp-device
>       :name     network
                :
```

b.
Confirm that the interface name that is obtained from the above operation matches the one that has been added to the PCI bus slot.

```
# /usr/sbin/FJSVmadm/inst2comp hme2 <Return>
pcipsy18:R0B01-PCI#slot02
```

c.
The configuration of each driver is added.
Please refer to each driver manual for details.

6) Connect to redundant system

Please execute following commands in order to connect the extended PCI card to the existing redundant configuration system.

Fast switching mode

```
# /usr/sbin/ifconfig hme2 plumb <Return>
# /usr/sbin/ifconfig hme2 IP_address netmask + broadcast + -trailers up <Return>
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i hme2 -f <Return>
```

GS/SURE linkage mode

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0 <Return>
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i IP_address -t hme2 <Return>
# /opt/FJSVhanet/usr/sbin/hanetnic modify -n sha0 -t sha2,sha3,sha4 <Return>
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0 <Return>
```

7) Switch the redundant path

Please switch an online communication path for extended communication path if needed.

8) Start the hardware monitoring of the Machine Administration

Please execute the following command in order to update configuration information, and restart the hardware monitoring of the Machine Administration.

```
# /usr/sbin/FJSVmadm/postphp <Return>
```

4.6 Recovery Procedure from Line Failure

This section explains the recovery procedure in various modes after a line failure has occurred.

4.6.1 Recovery procedure from line failure in Fast switching mode

No special operation is required because recovery is automatically made after a line failure has occurred.

However, some applications may need to be restarted.

4.6.2 Recovery procedure from line failure in RIP mode

The following shows the recovery procedure from a line failure in RIP mode.

Some applications may need to be restarted after the recovery procedure on Redundant Line Control function.

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

4.6.3 Recovery procedure from line failure in Fast switching/RIP mode

For information on the recovery procedure from a line failure in Fast switching/RIP mode, see Sections "4.6.1 Recovery procedure from line failure in Fast switching mode" and "4.6.2 Recovery procedure from line failure in RIP mode".

4.6.4 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
```

4.6.5 Recovery procedure from line failure in GS/SURE linkage mode

No special operation is required because recovery is automatically made after a line failure has occurred.

However, some applications may need to be restarted.

4.6.6 How to recover when an error occurred in a transfer route at the execution of DR

Described in this section is the recovery procedure from a transfer route error occurred during DR operation to replace a system board. After the recovery, execute "drc -connect" command and finish the DR operation.

[Fast switching mode]

See "4.6.1 Recovery procedure from line failure in Fast switching mode" as to how to recover when an error occurred in a transfer route in Fast switching mode.

[RIP mode]

See "4.6.2 Recovery procedure from line failure in RIP mode" as to how to recover when an error occurred in a transfer route in RIP mode.

[Fast switching/RIP mode]

See "4.6.3 Recovery procedure from line failure in Fast switching/RIP mode" as to how to recover when an error occurred in a transfer route in fast switching/RIP mode.

[NIC switching mode]

Regarding DR execution in NIC switching mode, because HUB monitoring function and standby patrol function stop while replacing a system board, network communication is suspended if a failure is detected in a transfer path. After recovering the transfer path, communication will be restored thus recovery process is not necessary.
Some applications may require reactivating the application.

[GS/SURE linkage mode]

See "4.6.5 Recovery procedure from line failure in GS/SURE linkage mode" as to how to recover when an error occurred in a transfer route in GS/SURE linkage mode.

4.6.7 How to recover when an error occurred in a transfer route at the execution of PHP

The following describes the recovery procedures from a failure occurred during NIC (PCI card) replacement operation with PHP.

[Fast switching mode]

See "4.6.1 Recovery procedure from line failure in Fast switching mode" as to how to recover when an error occurred in a transfer route in Fast switching mode.

[NIC switching mode]

While executing PHP, because HUB monitoring function and standby interface monitoring function stops while exchanging the NIC (PCI card), if a failure is detected in a transfer path, it suspends the network communication. After the transfer path recovers, the communication recovers as well, so no further recovery work is required. However, some application requires restarting the application.

[GS/SURE linkage mode]

See "4.6.5 Recovery procedure from line failure in GS/SURE linkage mode" as to how to recover when an error occurred in a transfer route in GS/SURE linkage mode.

As for RIP and Fast switching/RIP modes, there is no recovery procedure as PHP expansion/replacement mechanisms cannot be used in those modes.

4.7 Backing up and Restoring Configuration Files

This section explains how to back up and restore configuration files of Redundant Line Control function.

4.7.1 Backing up Configuration Files

Use the hanetbackup command to back up configuration files.

For details about this command, see Section "7.12 hanetbackup Command".

4.7.2 Restoring Configuration Files

Use the hanetrestore command to restore configuration files.

For details about this command, see Section "7.13 hanetrestore Command".

After executing this command, restart the system immediately. The system will not operate as defined in the configuration file, unless you reboot the system.

Chapter 5 GLS operation on cluster systems

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

5.1 Outline of Cluster System Support

In cluster system, Redundant Line Control function supports the following operation modes:

- Active standby system (1:1 and N:1)
- Mutual standby system
- Cascade system
- Priority transfer system

How cluster failover is dealt with in each mode is shown below.

Table 5.1 List of the cluster system compatible function

Mode	Active Standby System (1:1)	Active Standby System (N:1)	Mutual standby System	Cascade System	Priority transfer system	Duplicate transfer path for SIS
Fast switching mode	A	A	A	A	A	X
RIP mode	X	X	X	X	X	X
Fast Switching/RIP mode	X	X	X	X	X	X
NIC switching mode	A	A	A	A	A	A
GS/SURE linkage mode	A	X	X	X	X	X

[Meaning of the symbols] A: Supported X: Not supported

Virtual IP addresses allocated to virtual interfaces are taken over if a cluster switching event occurs. GLS does not provide any function to support MAC address takeover and system node name takeover. A physical interface used for GLS cannot be used to configure a cluster resource (Takeover IP address and Takeover MAC address). Table 5.2 indicates the support status of each takeover function.

Table 5.2 Supported cluster take over information

Cluster Operation mode	IP address	MAC address	IP address + MAC address	IP address + System node name	IP address + MAC address + System node name
1:1 Active standby	A	X	X	X	X
N:1 Active standby	A	X	X	X	X
Mutual standby	A	X	X	X	X
Cascade	A	X	X	X	X
Priority transfer	A	X	X	X	X

[Meaning of the symbols] A: Supported X: Not supported B: No match

- 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.
- Scalable configuration as well as standby configuration in High-availability scalable settings are not supported.
- When switching the node in both Fast Switching and NIC switching mode, do not use IPv6 address as a take over virtual interface if immediate communication is required. If IPv6 address is used, it takes approximately 30 seconds to restore communication after switching the node. For detail, see “D.2 Trouble shooting”.
- The logical virtual interface and IP address allocated in the Solaris zone cannot be taken over along with cluster switching. If a failure occurs on all the transmission routes of the operating node, a communication session between the Solaris zone and Global zone fails.

Figure 5.1 shows an example of cluster switching for the virtual interface.

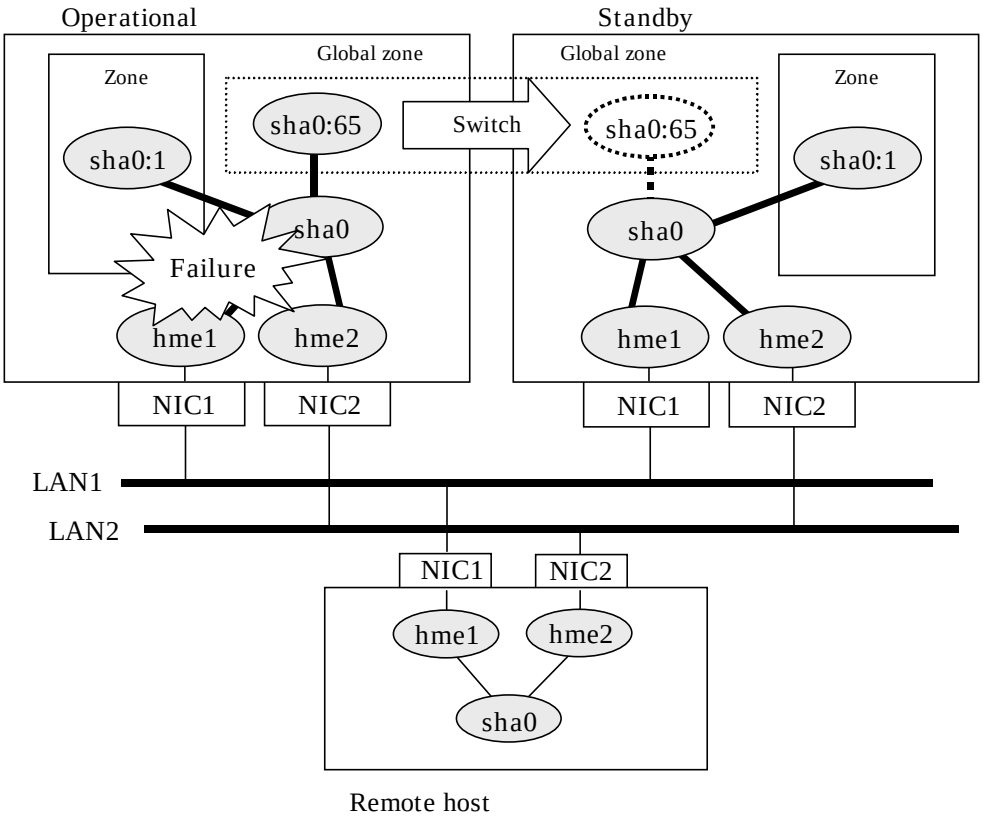


Figure 5.1 Cluster Switching for the virtual interface

The logical unit number for the virtual interface for cluster switching is 65 or later. (sha0:65, sha0:66)

5.1.1 Active Standby

5.1.1.1 Starting

5.1.1.1.1 Fast switching mode

With userApplication startup, the takeover virtual interface (sha0:65) over operating node will be activated, enabling communication using the takeover virtual IP address.

When operating, Fast switching mode uses the Redundant Line Control function to communicate with the remote system.

Note that the virtual interface (such as sha0) is inactive just after GLS starts up. The virtual interface will be active after the first startup of userApplication. Once it becomes active, regardless of stopping or restarting userApplication, it remains to be active until the system stops.

When communicating with the other network using the virtual interface of Fast switching mode, or activating the virtual interface prior to userApplication startup, use hanetparam command to set the activation timing.
For detail, refer to “7.6 hanetparam Command”.
For description of setup, refer to “D.1 Changing Methods of Activating and Inactivating Interface”.

Figure 5.2 shows behavior of Fast switching mode after starting up

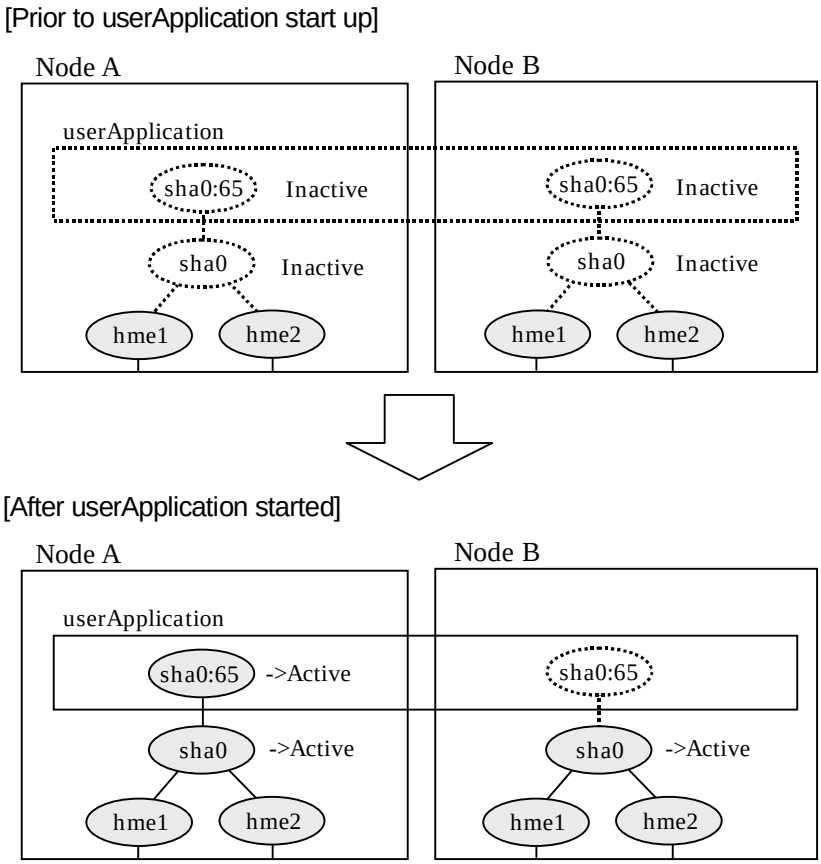


Figure 5.2 Startup behavior of Fast switching mode

5.1.1.1.2 NIC switching mode

NIC switching mode has the following address takeover functions. Select a function to be used depending on your operation.

- Logical address takeover
  Using the logical address takeover function allows a LAN to have several virtual IP addresses. Ordinary communication will be done via a physical IP address, and a communication through GLS will be done via the virtual IP addresses.
  For the remote system device to make a connection, a physical IP address should be specified as the connection address. Then, the remote system device can directly connect to the active or standby node and manage each of the nodes regardless of the status transition of the userApplication.
  For this function, two IP addresses are assigned to one physical interface. To use a TCP/IP application that requires only one IP address to be specified, use the physical address takeover function I or II.
- Physical IP address takeover I
  Use the Physical IP address takeover function I for a GLS network and an ordinary network to exist in a same LAN, sharing an IP address allocated to a physical interface. This function allows a connection to be made for each of the active and standby nodes independently. However, IP address of the standby node changes according to the status transition of the userApplication. Thus, when clusters are switched, the TCP connection to the standby node is cleared. For the communication target device to make a connection again, the connection IP address must be changed.
- Physical IP address takeover II
  Use the Physical IP address takeover function II to use a LAN only for GLS networking. In this case, no connection can be made to the standby node because the LAN of the standby node is inactivated. Another LAN must be provided to make a connection.

Figure 5.3 shows the active standby configuration diagram of duplicated operation in NIC switching mode (logical IP address takeover function). The operation in this figure is as follows: On active node A, the logical interface (hme1:1) of the secondary interface (hme1) is assigned the takeover virtual IP address (IP-A) and activated. If switching occurs due to a failure, the takeover virtual interface (hme1:1) that has been assigned the takeover IP address (IP-A) is inactivated. Then, on standby node B, the logical interface (hme0:1) that has been assigned the takeover IP address (IP-A) on the already activated primary interface (hme0) is activated.

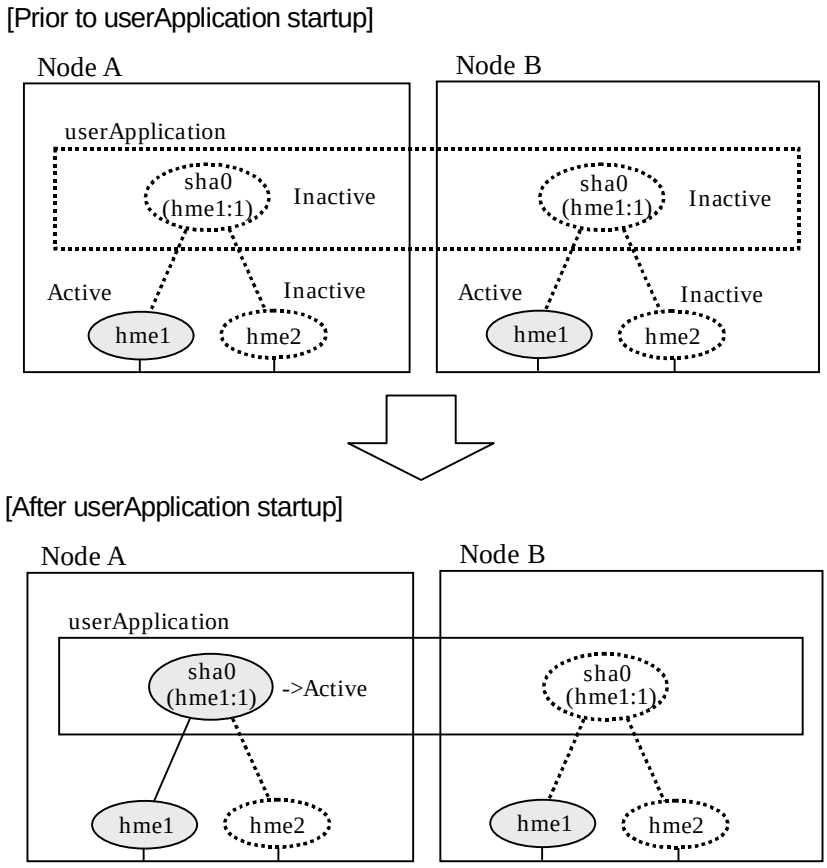


Figure 5.3 Startup behavior of NIC switching mode (take over logical IP)

For taking over physical IP address I, activate the physical interface (hme1) for operating node and standby node when the Redundant Line Control function starts up. After the userApplication starts, it will activate the physical interface by allocating a takeover IP address to the physical interface on the operating node. At this time, a physical interface (hme1) over the standby node remains to be inactive.

Figure 5.4 shows a startup behavior of takeover physical IP address I

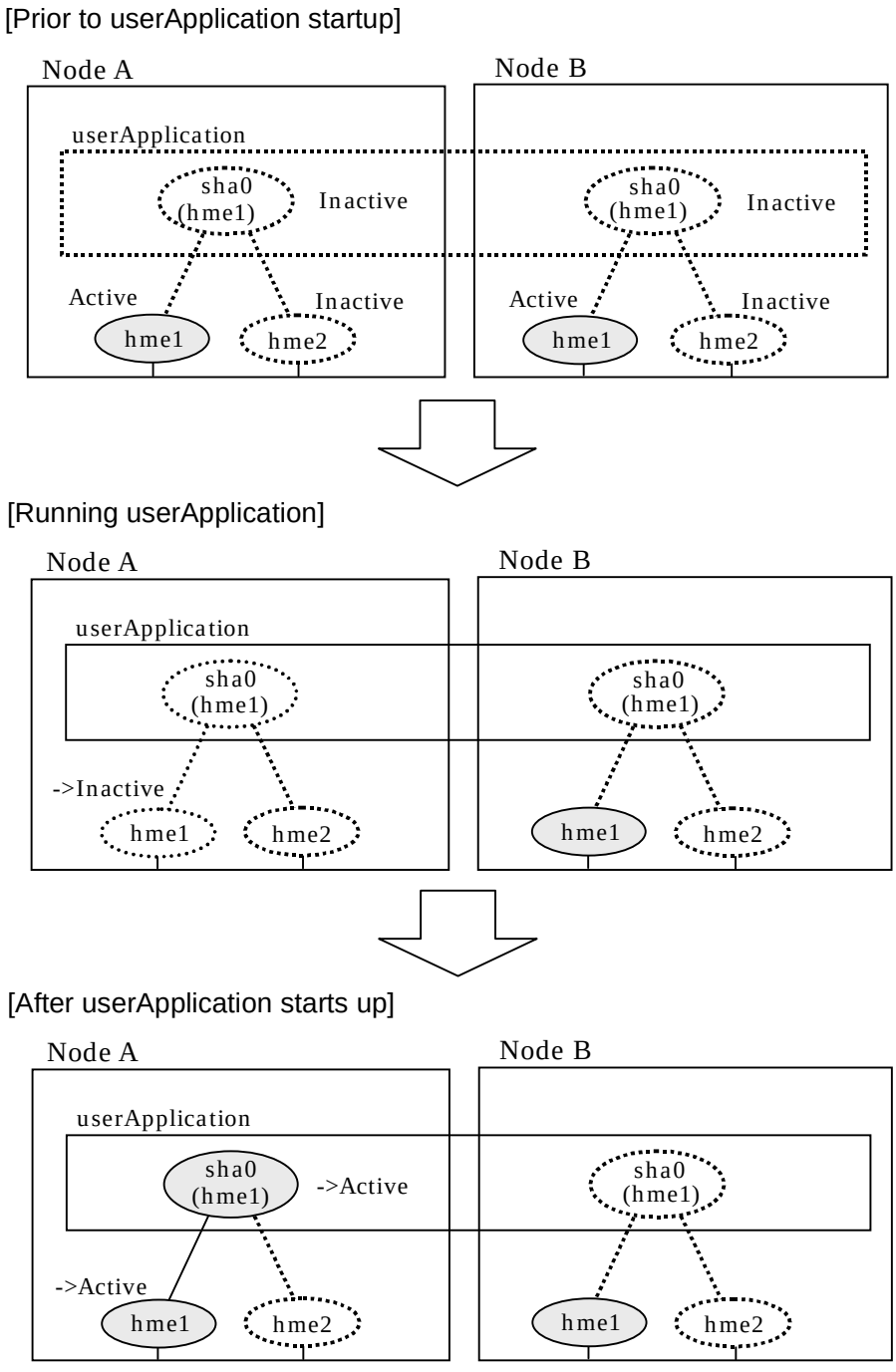


Figure 5.4 Startup behavior of NIC switching mode (takeover physical IP address I)

For taking over physical IP address II, it does not activate the physical interface (hme1) for both operating node and standby node when Redundant Line Control function starts up. Instead it allocates a takeover IP address to the physical interface (hme1) on the operating node and then it activates the physical interface. In this case, the physical interface (hme1) for standby node remains inactive.

Figure 5.5 shows a startup behavior of the takeover physical IP address II

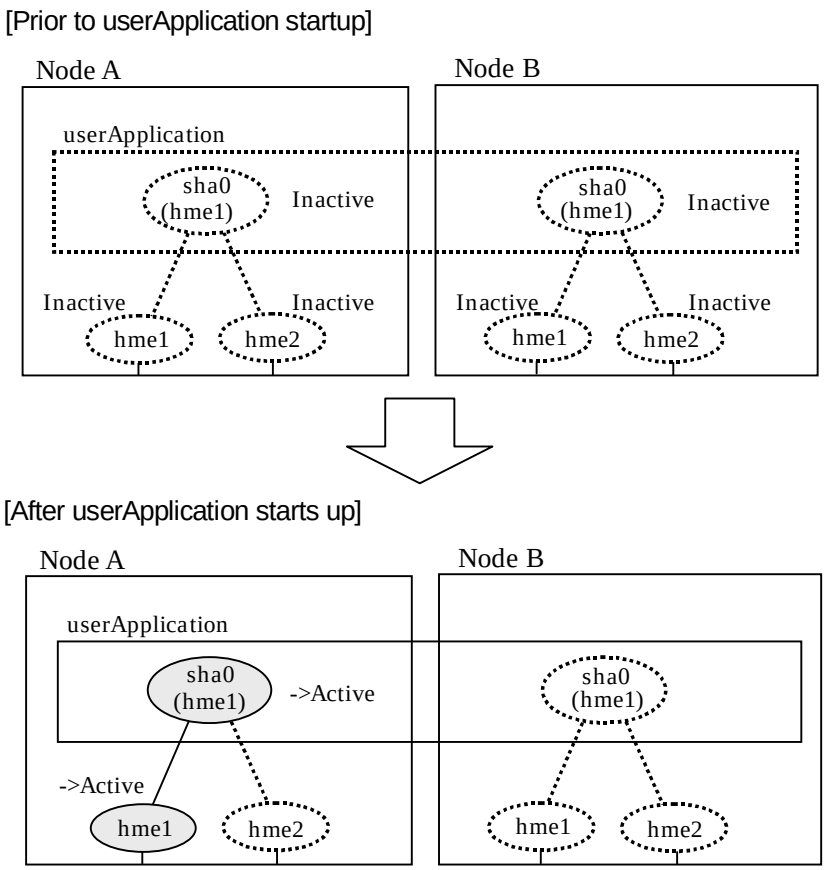


Figure 5.5 Startup behavior of NIC switching mode (takeover physical IP address II)

5.1.1.1.3 GS/SURE linkage mode

By starting userApplication, the take over virtual interface (sha0) over operating node becomes active allowing communication using the take over virtual IP address. When operating, GS/SURE linkage mode uses the Redundant Line Control function to communicate with the remote system.

Figure 5.6 shows startup behavior of GS/SURE linkage mode

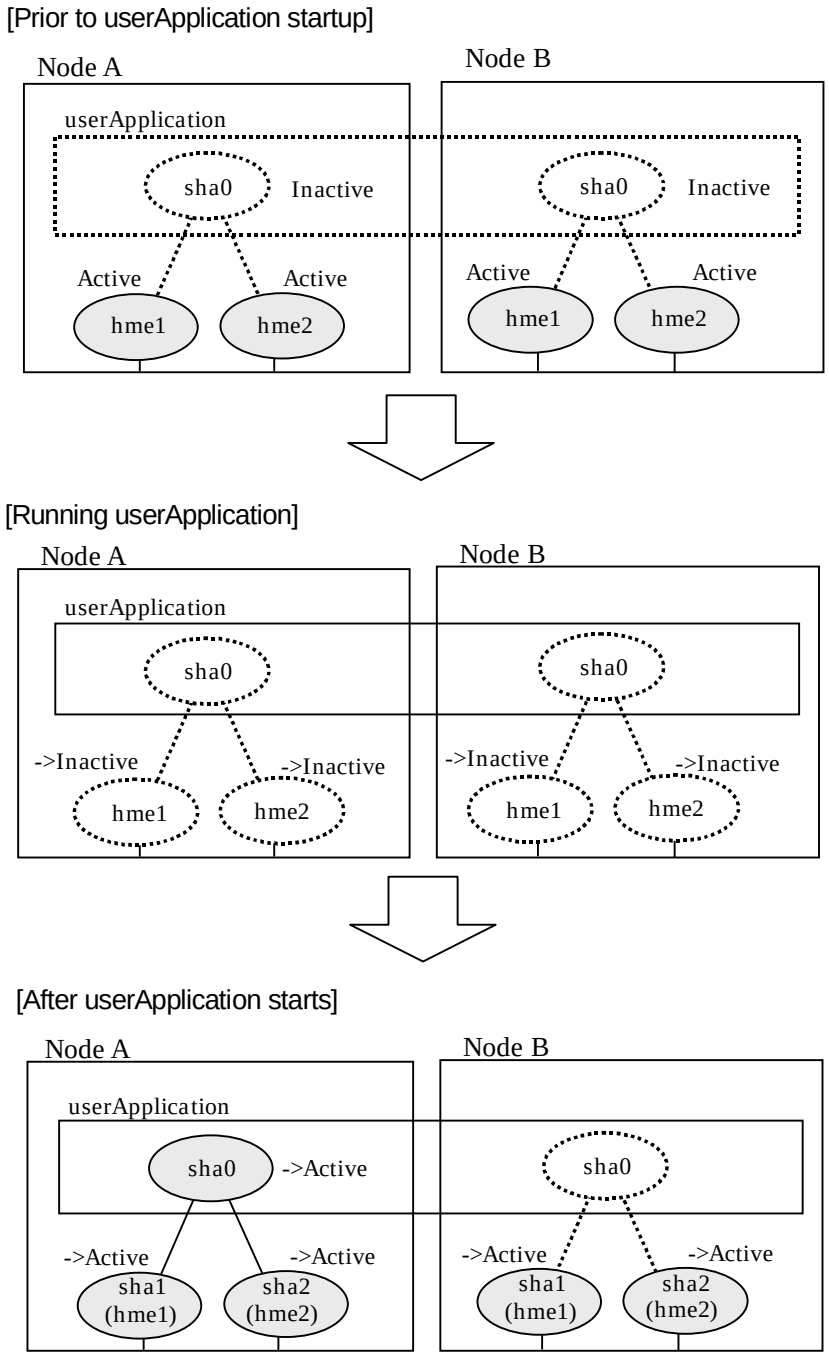


Figure 5.6 Startup behavior of GS/SURE linkage mode

5.1.1.2 Switching

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

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

5.1.1.2.1 Fast switching mode

Figure 5.7 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.

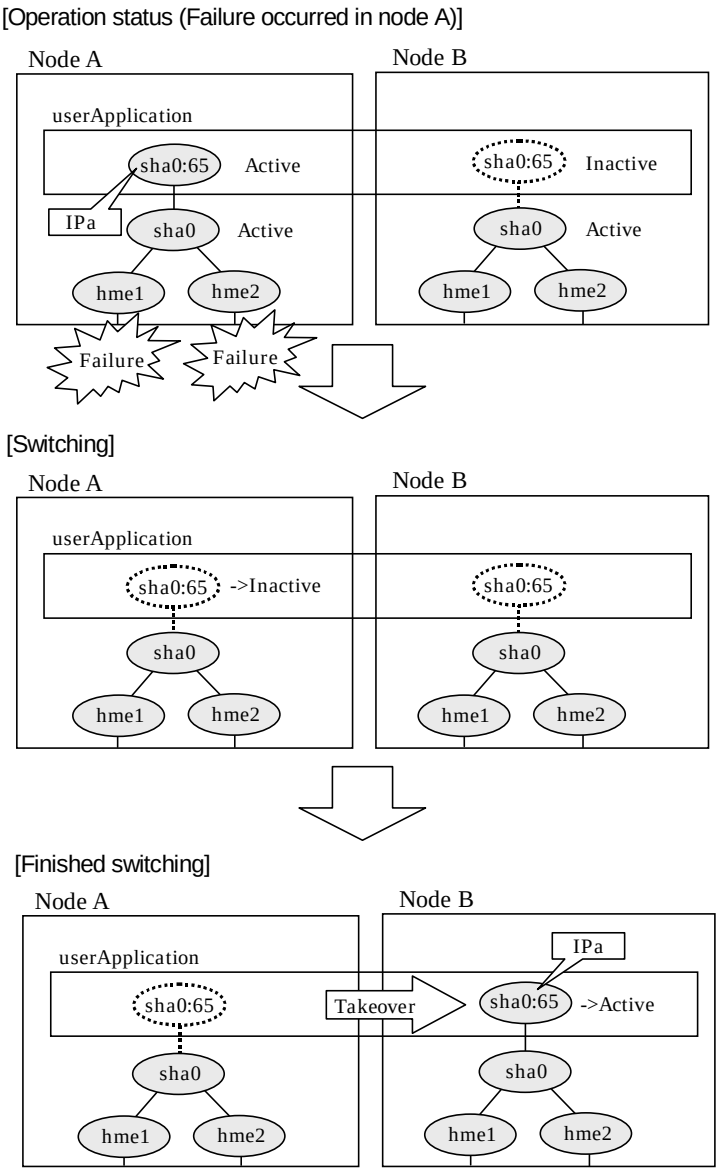


Figure 5.7 Switching behavior of Fast switching mode

5.1.1.2.2 NIC switching mode

Figure 5.8 illustrates switching behavior of NIC switching mode (logical IP address takeover function).

In the following figure, the takeover virtual IP address (IPa) in the operating node A is allocated to the logical interface (hme2.1) for the secondary interface. Once IPa is allocated, the logical interface (hme2.1) for the secondary interface turns into activate state.

When switching the node due to failure in the transfer routes, NIC switching mode inactivates the logical virtual interface which has allocated the takeover IP address (IPa) in the operating node A. Then it allocates the takeover IP address to the primary interface (hme1) and finally activates the logical interface (hme1:1).

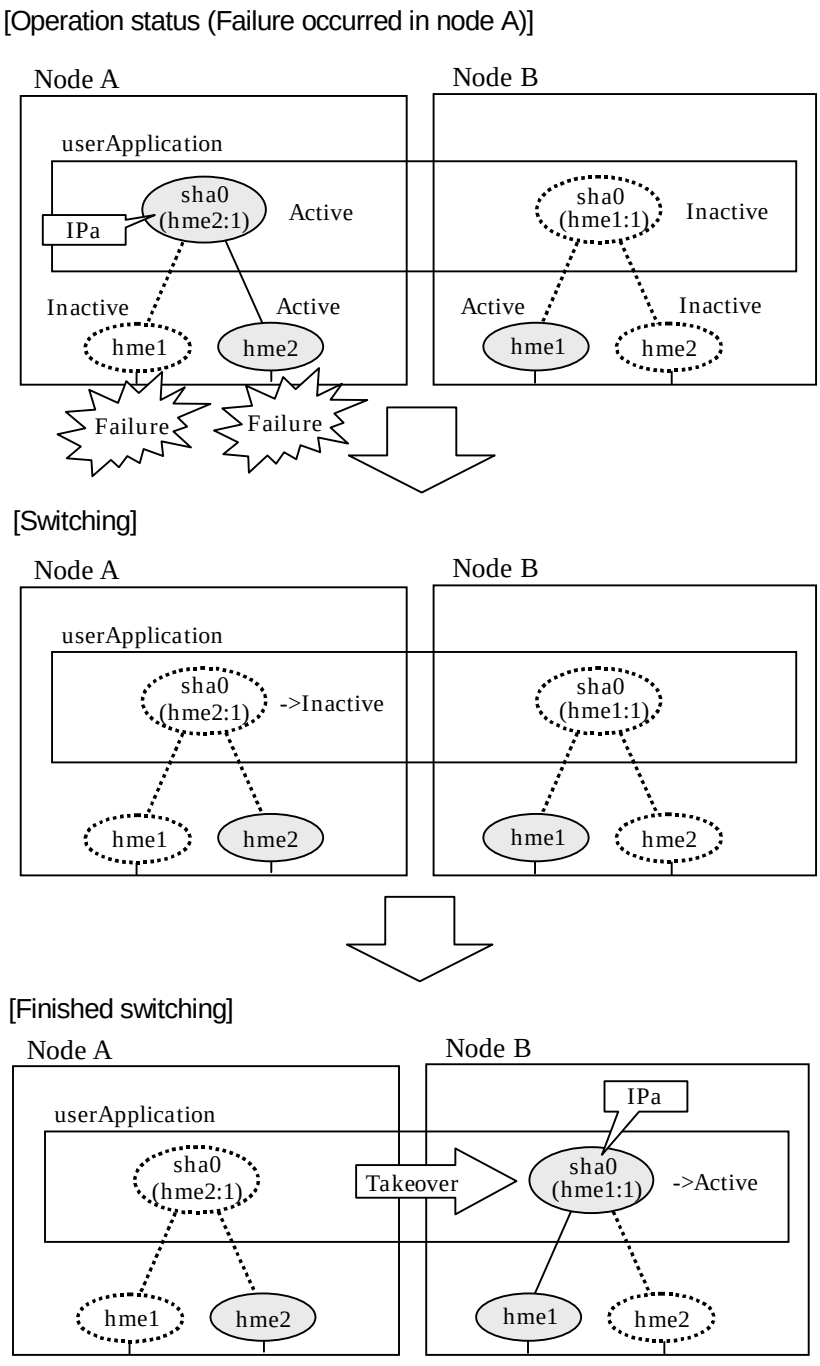


Figure 5.8 Switching behavior of NIC switching mode (takeover logical IP)

Figure 5.9 illustrates switching behavior of NIC switching mode (takeover physical IP address I).

In the following figure, the takeover virtual IP address (IPa) in the operating node A is allocated to the secondary interface. Once IPa is allocated it turns into activate state.

When switching the node due to a failure in the transfer routes, temporally inactivate the primary interface (hme1), which has been active in the standby node B. Then it allocates the takeover IP address (IPa) to activate the primary interface (hme1). Once the primary interface activates, different IP address is allocated to the secondary interface (hme2) by means of inactivating hme2.

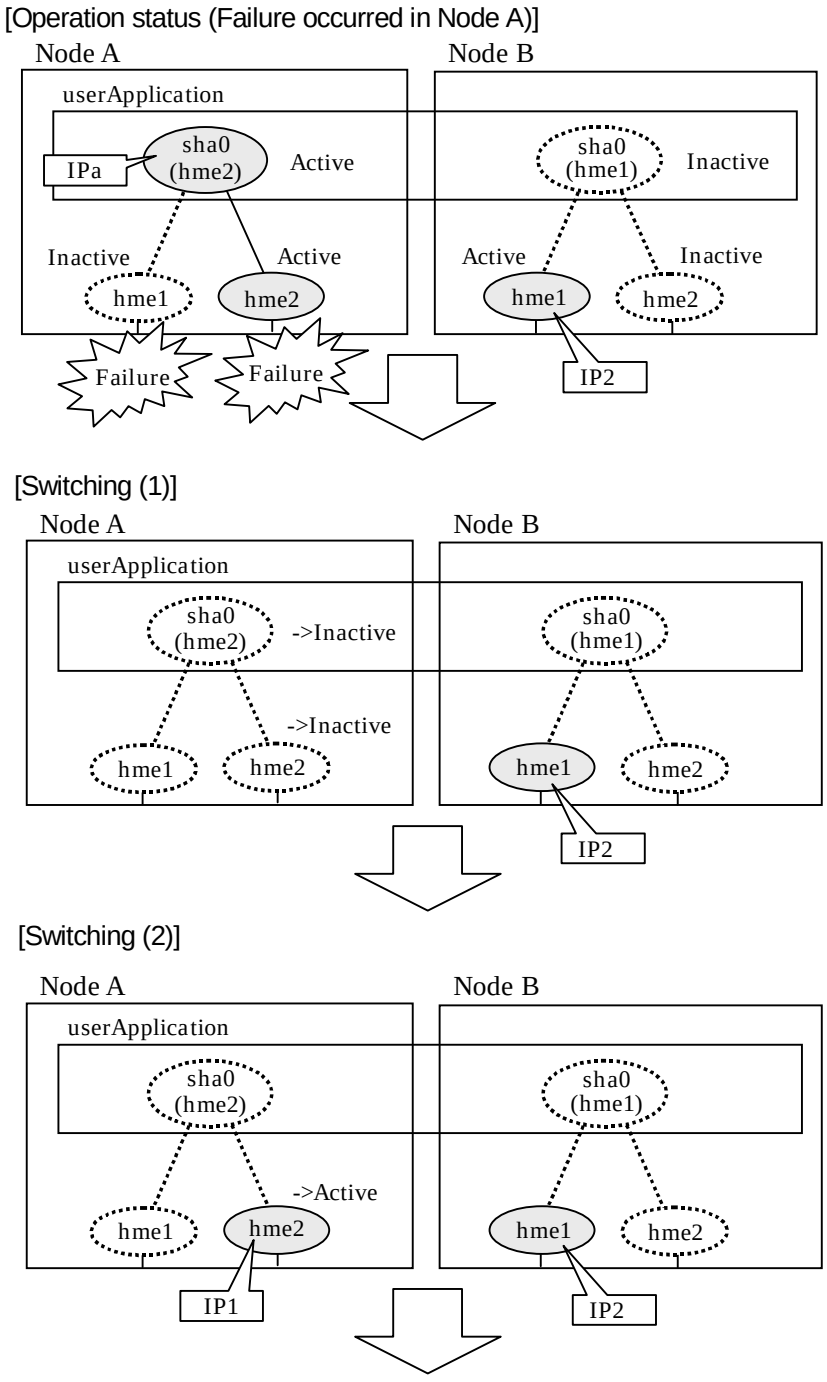


Figure 5.9 Switching behavior of NIC switching mode (takeover physical IP I) (continues)

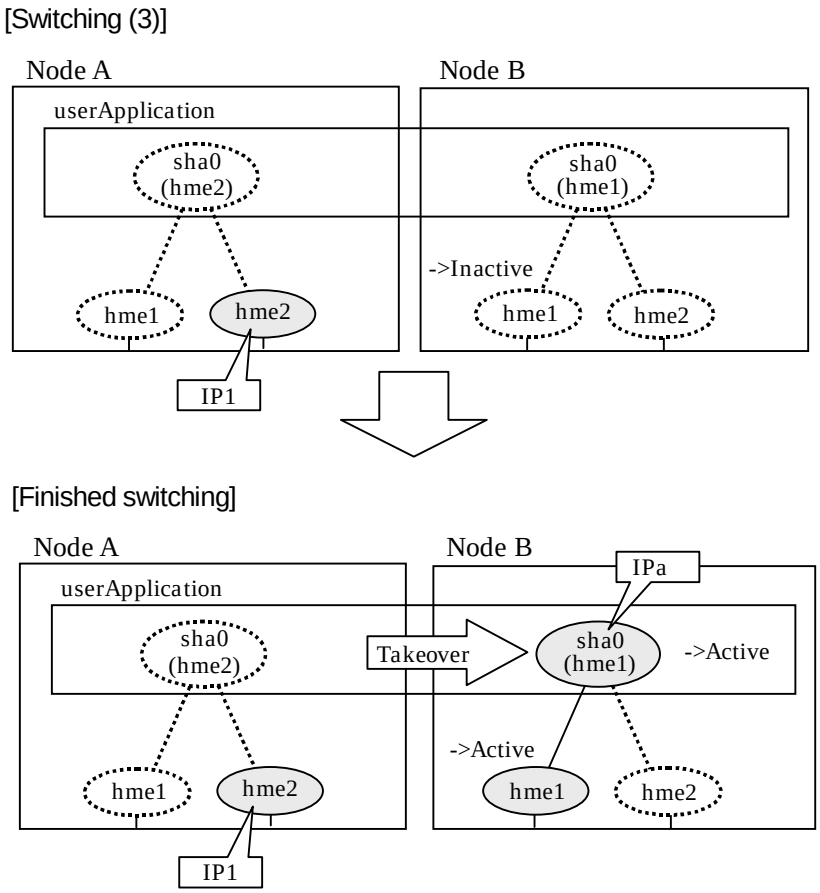


Figure 5.9 Switching behavior of NIC switching mode (takeover physical IP I)

Figure 5.10 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 (hme1). After the IP address is successfully passed over to the standby node, the secondary interface (hme2), which previously owned the takeover IP address (IPa) in node A becomes inactive.

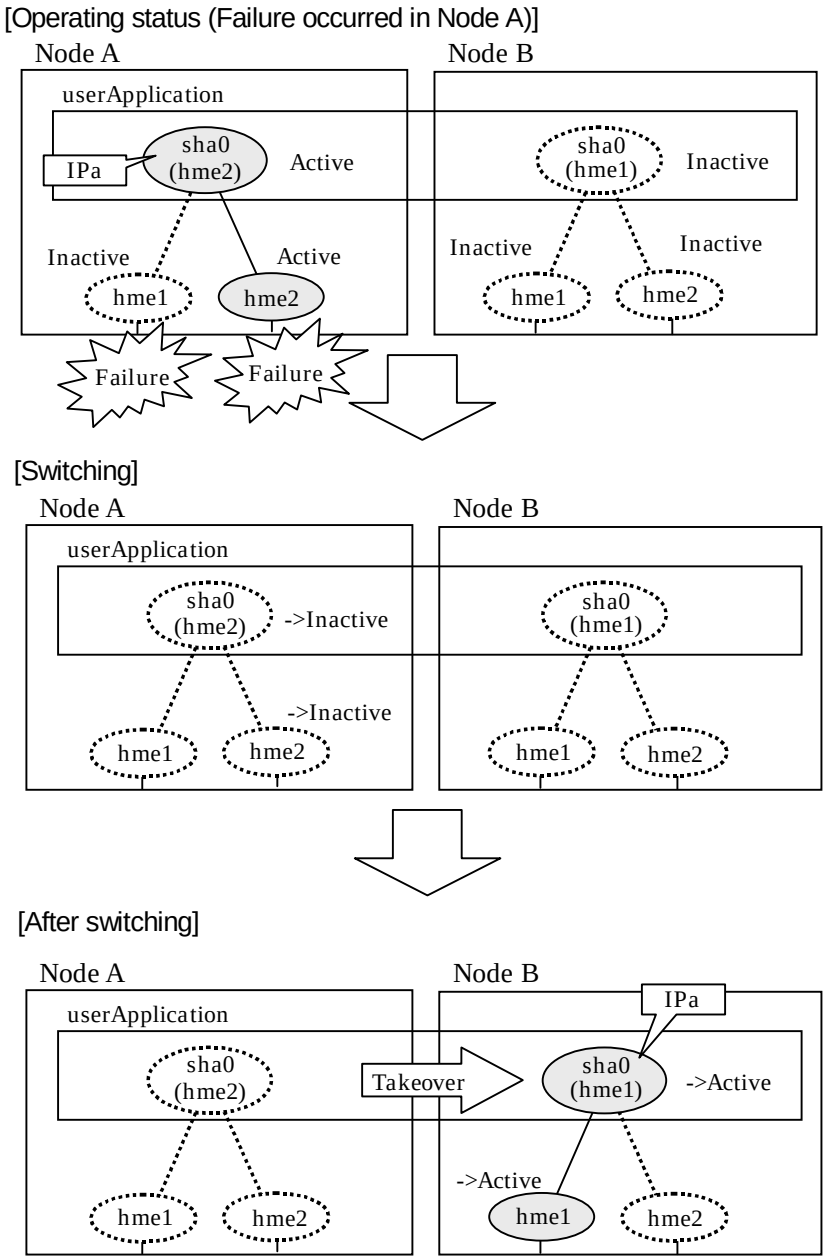


Figure 5.10 Switching behavior of NIC switching mode (takeover physical IP address II)

5.1.1.2.3 GS/SURE linkage mode

Figure 5.11 illustrates switching behavior of GS/SURE linkage mode.

In the figure below, a takeover virtual interface (sha0) is activated in the operating node. When switching occurs due to a failure, deactivate takeover virtual interface (sha0) and the virtual interfaces (sha1, sha2) in node A. Then, GS/SURE linkage mode activates the virtual interfaces (sha1, sha2). On standby node B, it activates the takeover virtual interface (sha0), which bundles the virtual interfaces (sha1, sha2).

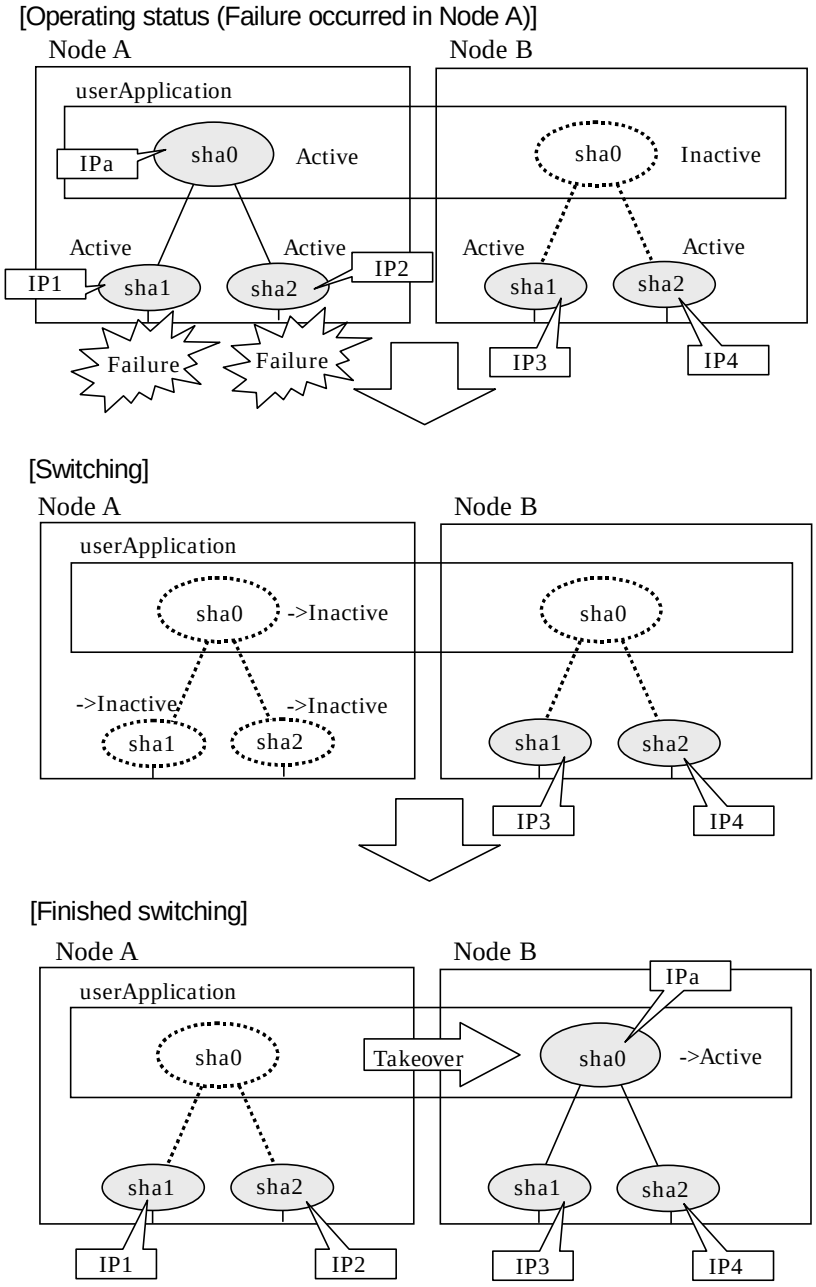


Figure 5.11 Switching behavior of GS/SURE linkage mode

5.1.1.3 Fail-back

The following shows a procedure of performing fail-back after failure recovery if node switching occurs.

1) Make recovery for a node on which a failure has occurred.

If switching has occurred due to panic or hang-up, reboot the node that has panicked or hanged up.
If switching has occurred due to a line failure, restore the line to a normal status (perform necessary work such as reconnecting a cable, powering on a HUB again, and replacing a faulty HUB).

2) Restore the original operation status.

Restore the original operation status by performing fail-back operation for userApplication.

5.1.1.4 Stopping

5.1.1.4.1 Fast switching mode

Figure 5.12 illustrates stopping process of userApplication.

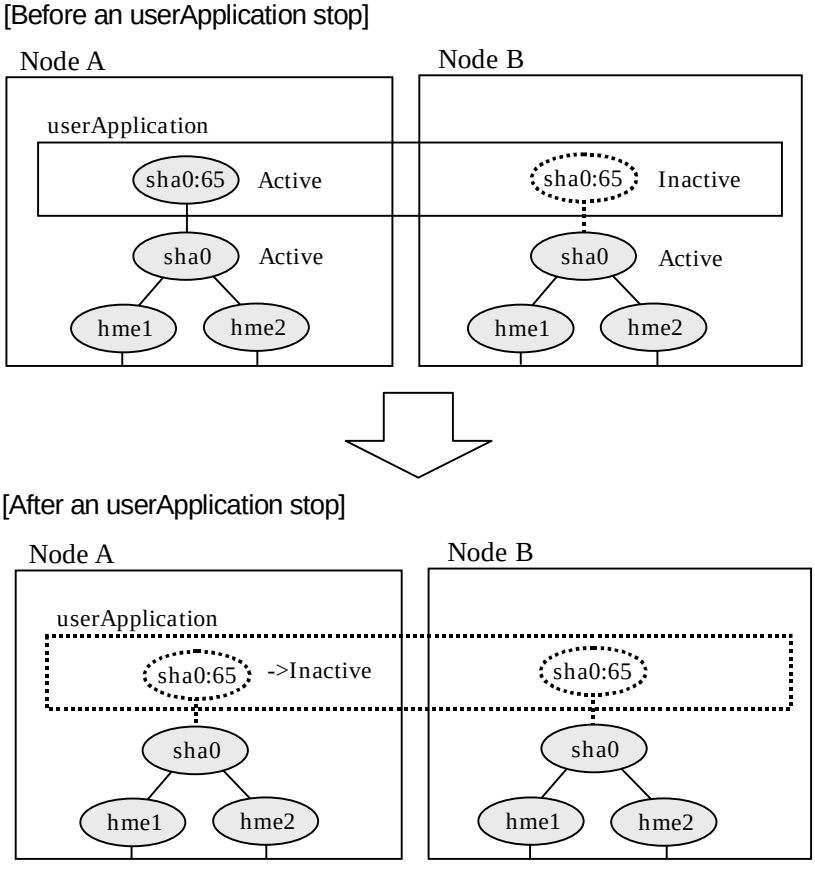


Figure 5.12 Stopping behavior of Fast switching mode

5.1.1.4.2 NIC switching mode

Figure 5.13 illustrates stopping process of userApplication for logical IP takeover.

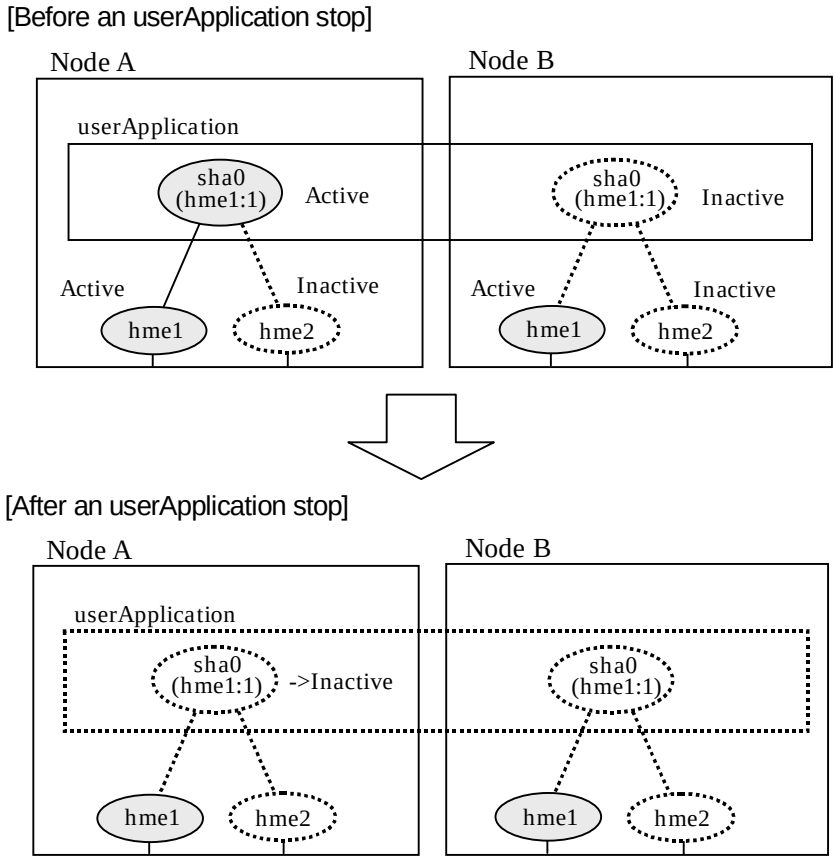


Figure 5.13 Stopping process of NIC switching mode (logical IP takeover)

Figure 5.14 illustrates stopping behavior of userApplication for the physical IP takeover I.

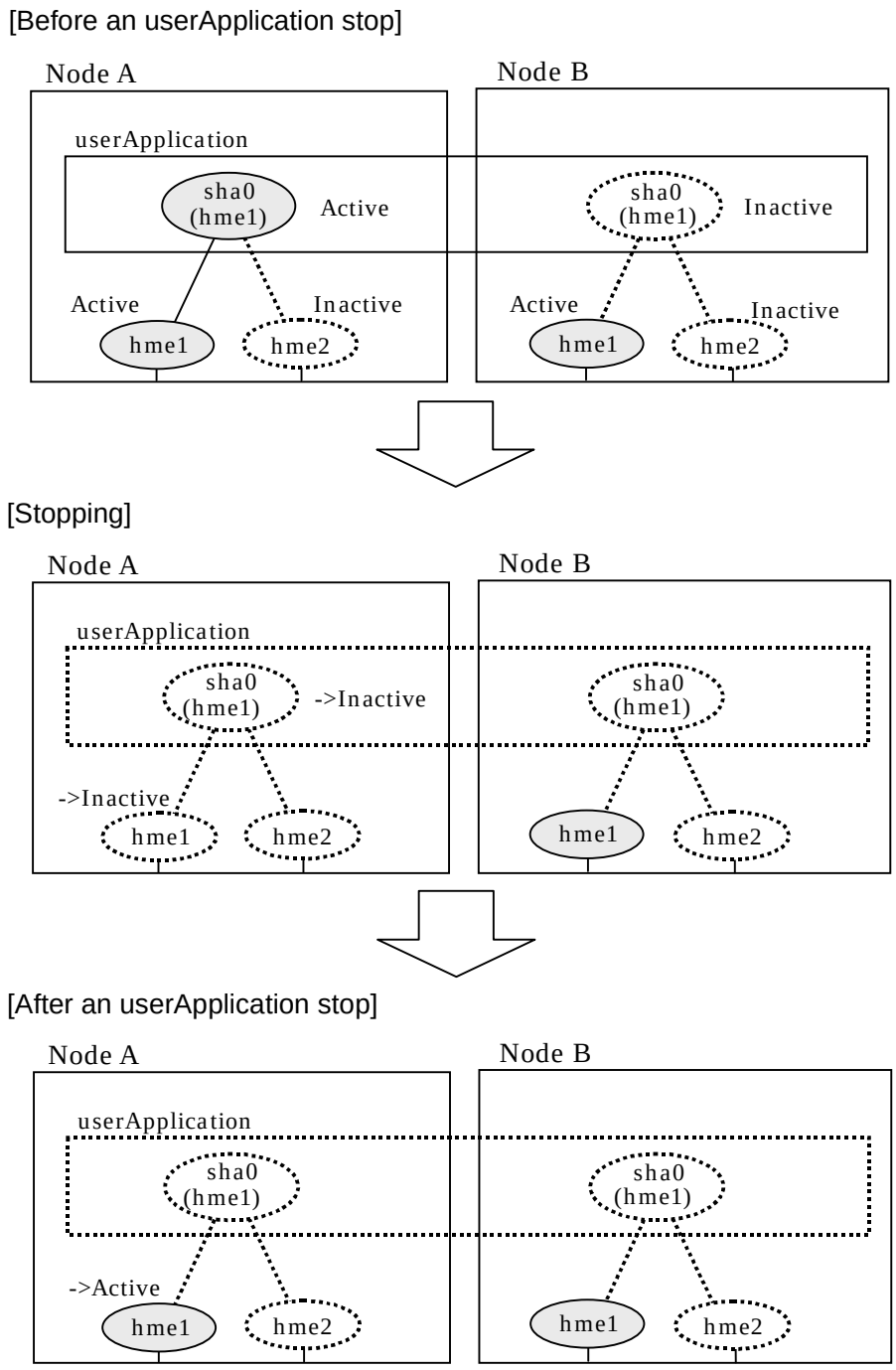


Figure 5.14 Stopping process of NIC switching mode (physical IP takeover)

Figure 5.15 illustrates stopping behavior of userApplication for the physical IP takeover II.

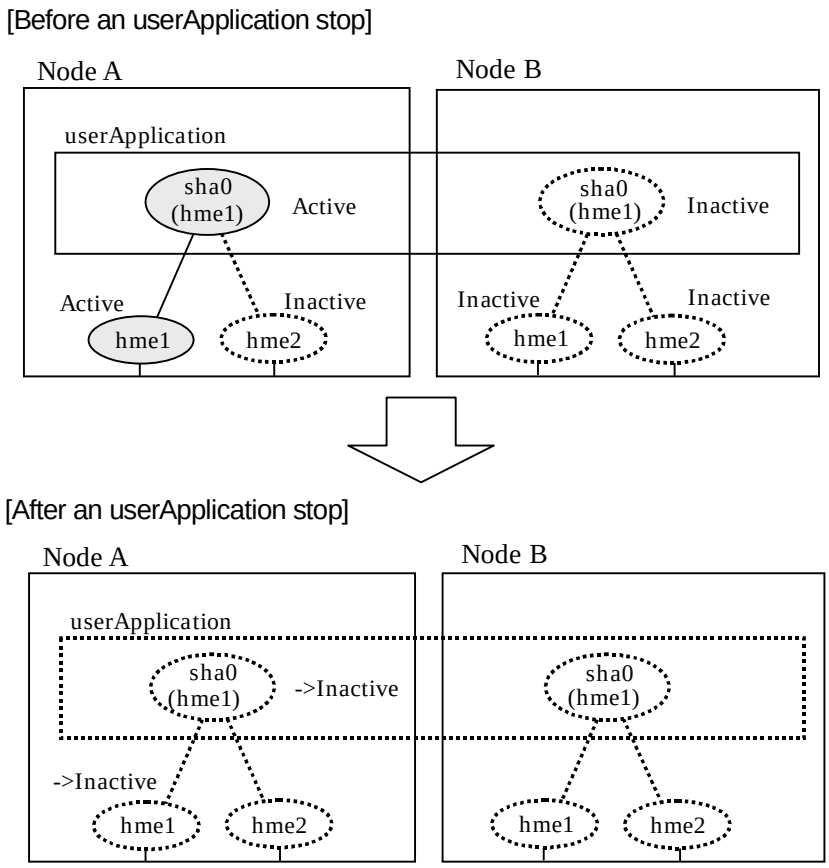


Figure 5.15 Stopping process of NIC switching mode (physical IP takeover II)

5.1.1.4.3 GS/SURE linkage mode

Figure 5.16 illustrates stopping behavior of userApplication.

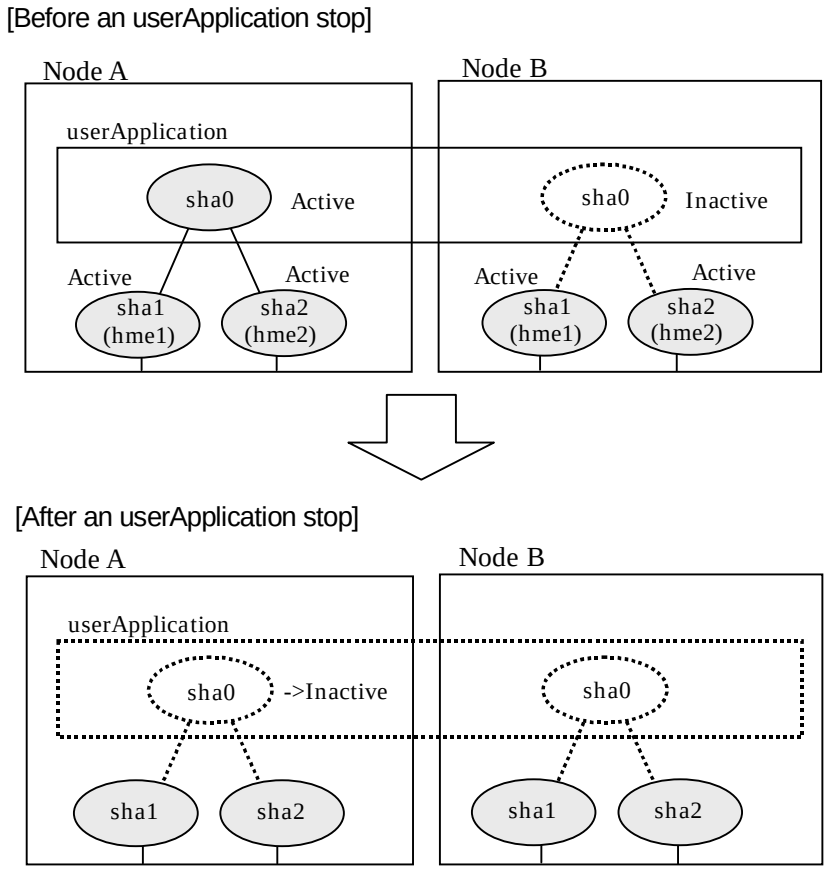


Figure 5.16 Stopping process of GS/SURE linkage mode

5.1.2 Mutual standby

A mutual standby operation can be achieved by defining several virtual interfaces and by configuring each resource as a separate userApplication.

5.1.2.1 Starting

Starting process is equivalent to the standby operation, except that the mutual standby operation contains various userApplications. For details, please refer to "5.1.1.1 Starting".

5.1.2.2 Switching

Usually, userApplication communicates with the remote system using the virtual interface on each node. If a failure (such as panic, hang-up, or transfer path failure) occurs on the operating node, the virtual interface comprised in that corresponding node is passed over to the standby node. With an application allowing reconnection, it takes over the connection of the operating node.

5.1.2.2.1 Fast switching mode

Figure 5.17 shows the mutual standby configuration diagram of duplicated operation in Fast switching mode. The takeover of an address, etc. is performed in the same way as for the active standby configuration. For information, see Section "5.1.1.1.1 Fast switching mode".

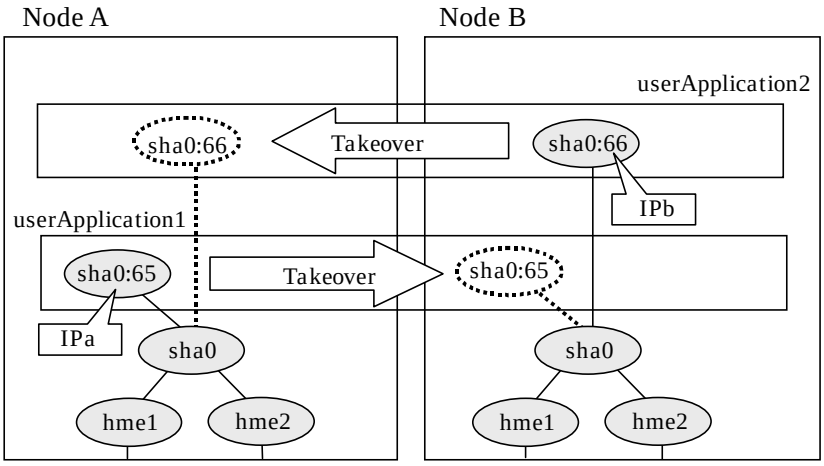


Figure 5.17 Mutual standby configuration diagram in Fast switching mode

5.1.2.2.2 NIC switching mode

Figure 5.18 shows the mutual standby configuration diagram in NIC switching mode (NIC non-sharing). The takeover of an address, etc. is performed in the same way as for the active standby configuration. For information, see Section "5.1.1.1.2 NIC switching mode".

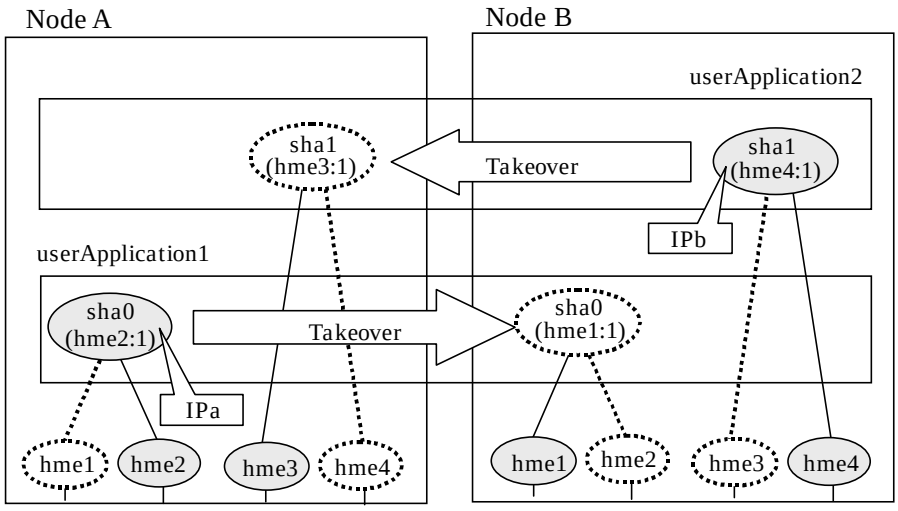


Figure 5.18 Mutual standby configuration diagram in NIC switching mode (NIC non-sharing)

Figure 5.19 shows the mutual standby configuration diagram in NIC switching mode (NIC sharing). The takeover of an address, etc. is performed in the same way as for the active standby configuration. For information, see Section "5.1.1.1.2 NIC switching mode".

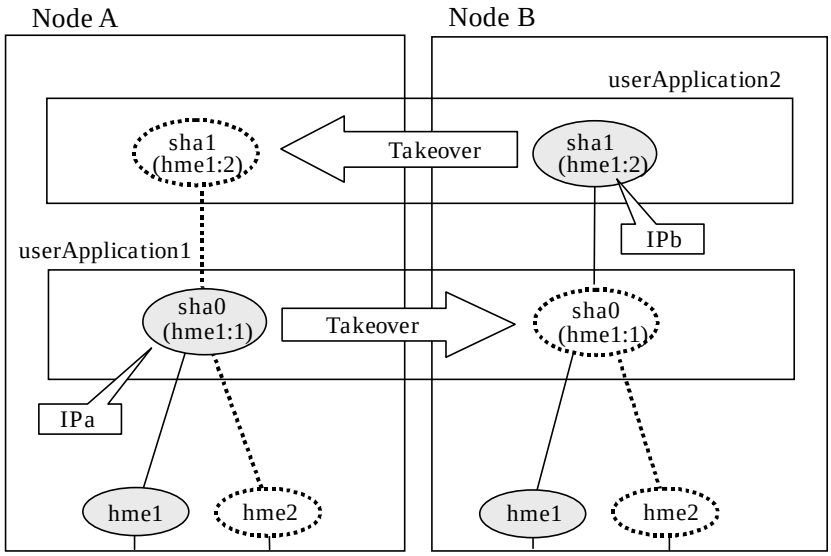


Figure 5.19 Mutual standby configuration diagram in NIC switching mode (NIC sharing)

5.1.2.3 Fail-back

The fail-back is performed in the same way as for the active standby configuration. For more information, see "5.1.1.3 Fail-back".

5.1.2.4 Stopping

Stopping operation is equivalent to active standby connection. For detail, see “5.1.1.4 Stopping”.

5.1.3 Cascade

5.1.3.1 Startup

5.1.3.1.1 Fast switching mode

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

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

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

Figure 5.20 illustrates start-up behavior of Fast switching mode

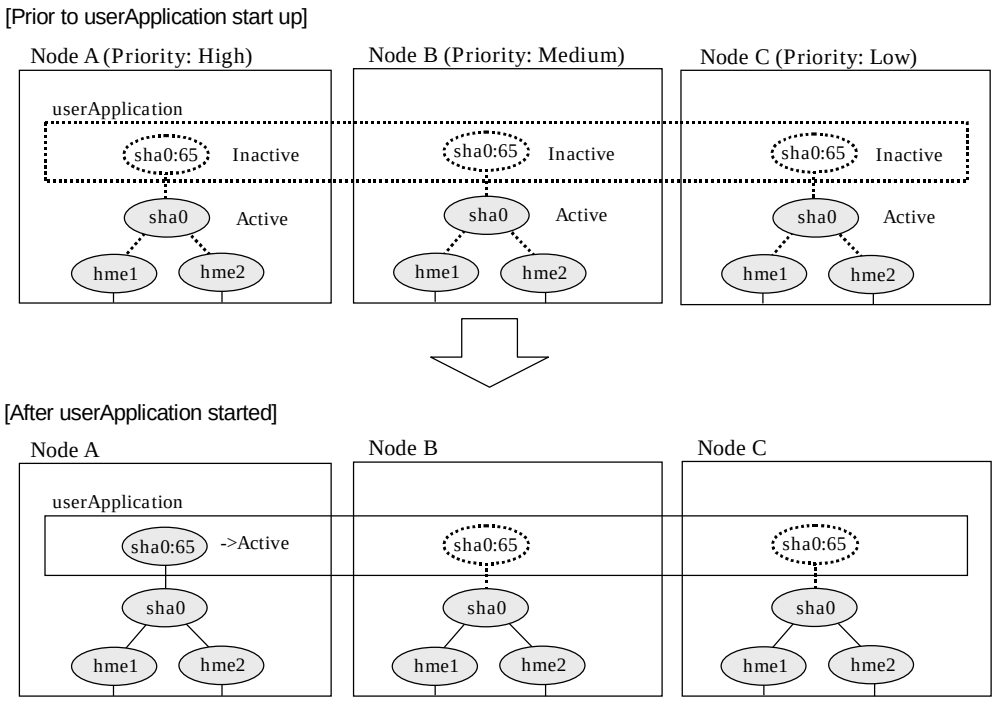


Figure 5.20 Start-up behavior of Fast switching mode

5.1.3.1.2 NIC switching mode

There are three types of IP takeover feature in NIC switching mode. For detail, refer to "5.1.1.1.2 NIC switching mode".

The physical interface (hme1) for each node becomes active when the redundant control function starts up for logical IP takeover. Once the userApplication starts up, takeover virtual interface (hme1:1) then becomes active on the operating node which has higher priority.

Figure 5.21 illustrates start-up behavior of logical IP takeover.

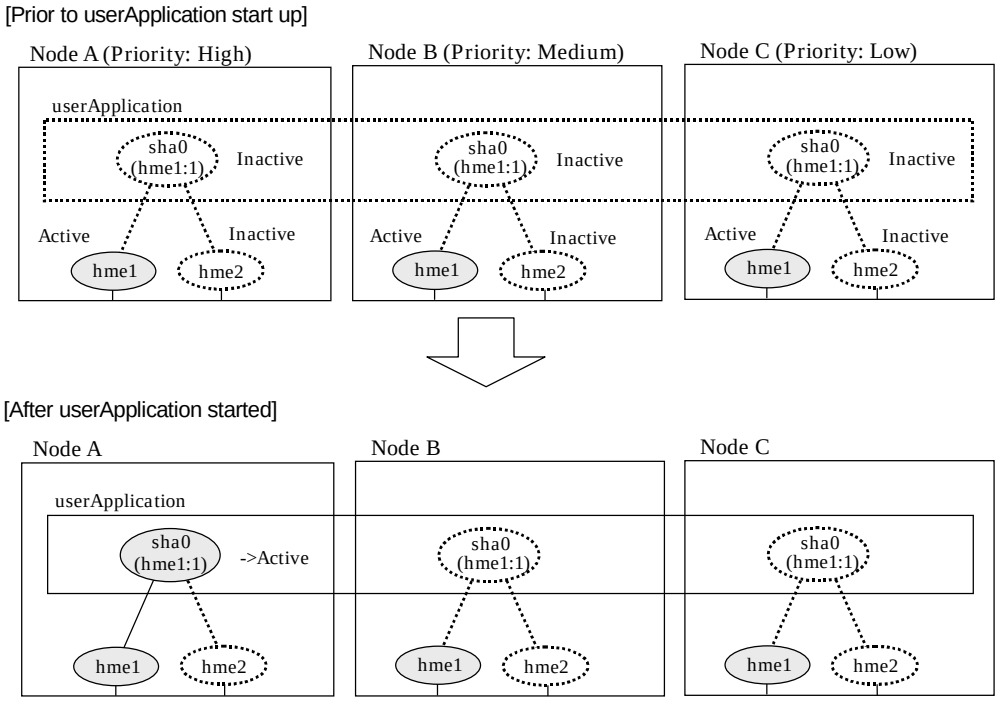


Figure 5.21 Start-up behavior of NIC switching mode (logical IP takeover)

The physical interface (hme1) for each node becomes active when the redundant control function starts up for the physical IP takeover I. Once the userApplication starts up, it activates the physical interface (hme1) by allocating the takeover IP address to the physical interface (hme1) on the operating node, which has a higher priority. During this process, the physical interface (hme1) on the standby node maintains its state.

Figure 5.22 illustrates start-up behavior of the physical IP takeover I.

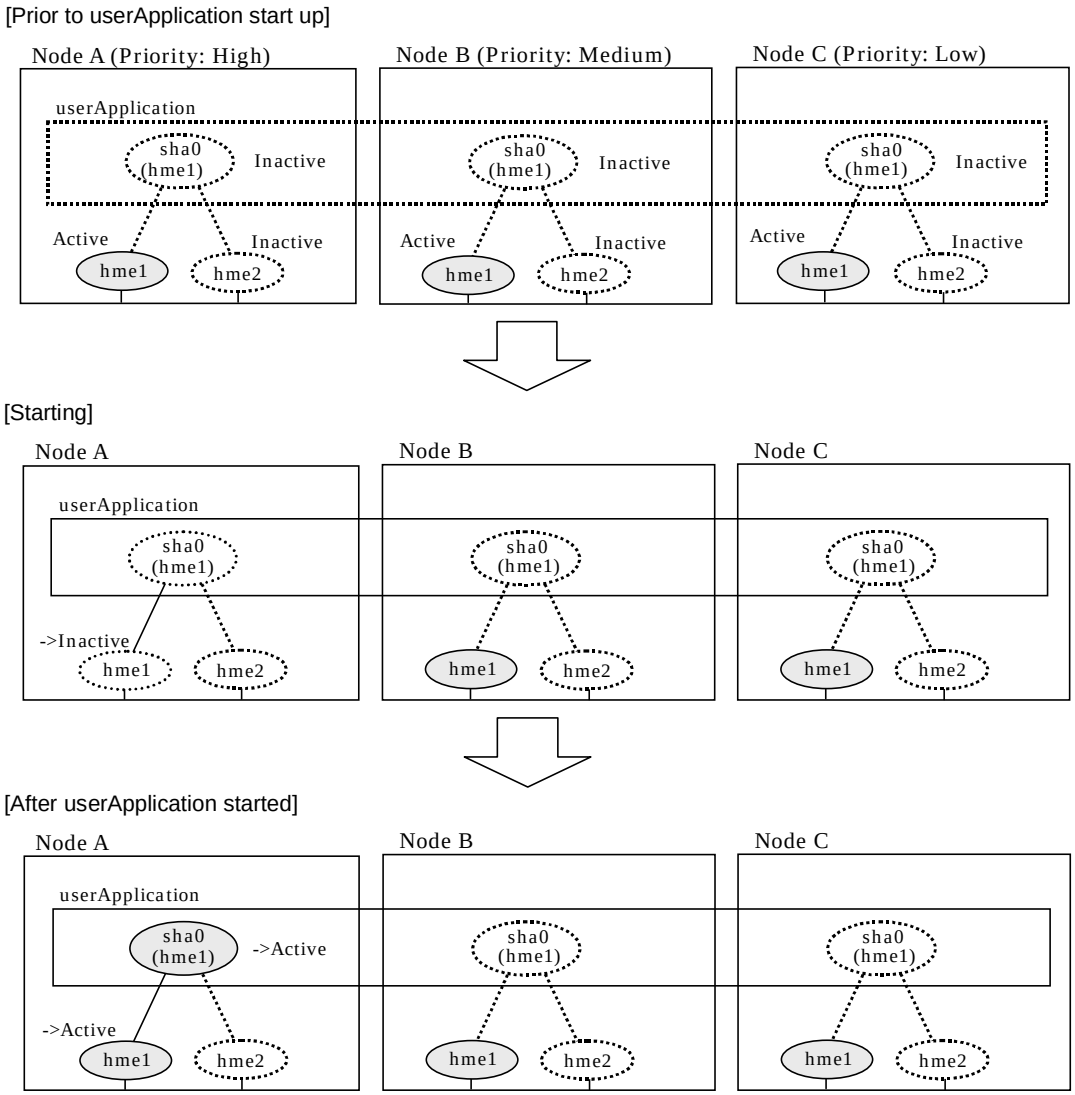


Figure 5.22 Start-up behavior of NIC switching mode (physical IP takeover)

The physical interface (hme1) for each node stays to be inactive when the redundant control function starts up for the physical IP takeover II. Once the userApplication starts up, it activates the physical interface (hme1) by allocating the takeover IP address to the physical interface (hme1) on the operating node, which has a higher priority. While this process takes place, the physical interface on the standby node remains inactive.

Figure 5.23 illustrates start-up behavior of physical IP takeover II

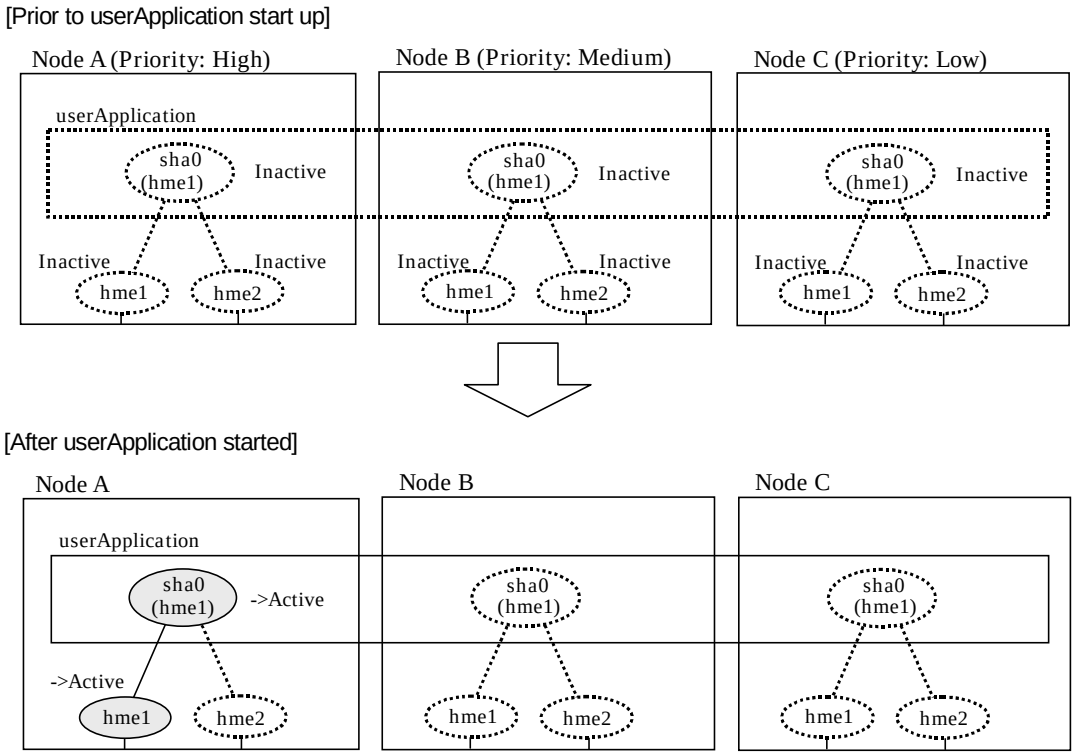


Figure 5.23 Start-up behavior of NIC switching mode (physical IP takeover II)

5.1.3.2 Switching

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

When a failure (panic, hang, detecting failure in transfer route) occurs in the operating node, redundant control function allows switching to the standby node, which has a higher priority within a several other standby nodes. It inherits the communication of operating node by reconnecting to the node using the application.

5.1.3.2.1 Fast switching mode

Figure 5.24 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.

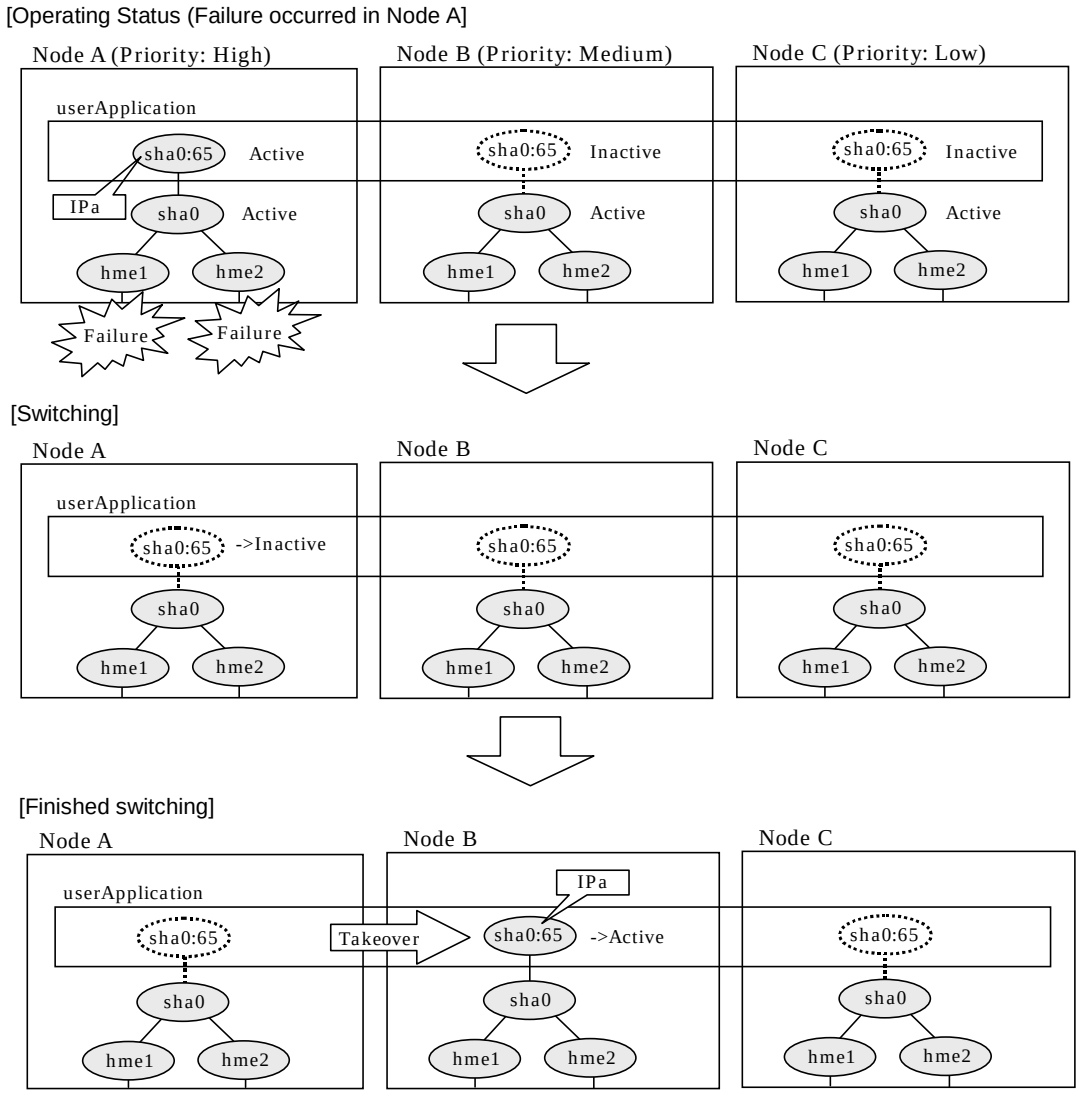


Figure 5.24 Switching operation of Fast switching mode

5.1.3.2.2 NIC switching mode

Figure 5.25 illustrates switching behavior of NIC switching mode (logical IP address takeover function).

In the following figure, the takeover virtual IP address (IPa) in the operating node A is allocated to the logical interface (hme2.1) for the secondary interface. Once IPa is allocated, the logical interface (hme2.1) for the secondary interface turns into activate state.

When switching the node due to failure in the transfer routes, NIC switching mode inactivates the logical virtual interface which has allocated the takeover IP address (IPa) in the operating node A. Then it allocates the takeover IP address to the primary interface (hme1) and finally activates the logical interface (hme1:1).

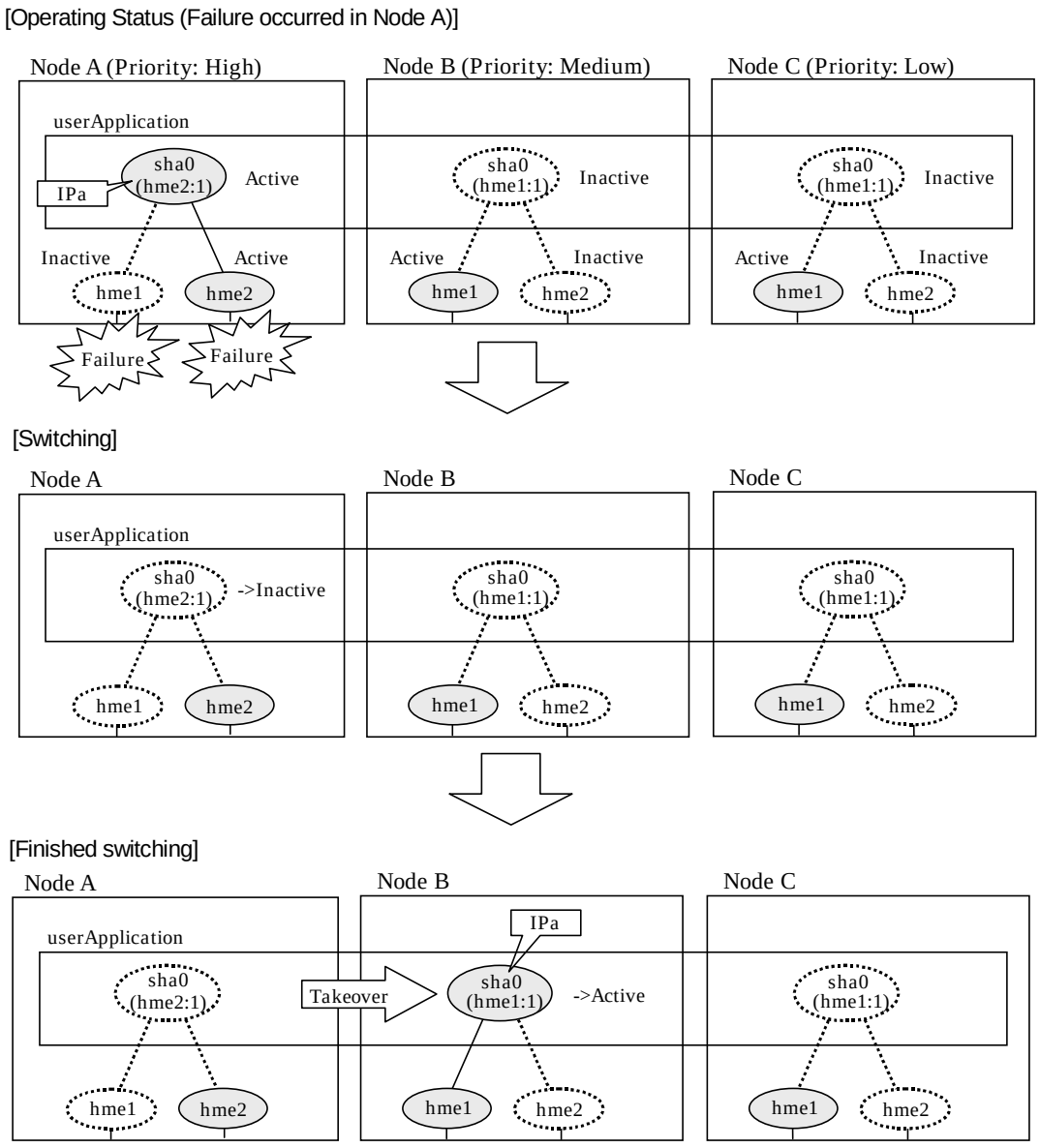


Figure 5.25 Switching operation of NIC switching mode (logical IP takeover)

Figure 5.26 illustrates switching behavior of NIC switching mode (takeover physical IP address I).

In the following figure, the takeover virtual IP address (IPa) in the operating node A is allocated to the secondary interface. Once IPa is allocated it turns into activate state.

When switching the node due to a failure in the transfer routes, temporally inactivate the primary interface (hme1), which has been active in the standby node B. Then it allocates the takeover IP address (IPa) to activate the primary interface (hme1). Once the primary interface activates, different IP address is allocated to the secondary interface (hme2) by means of inactivating hme2.

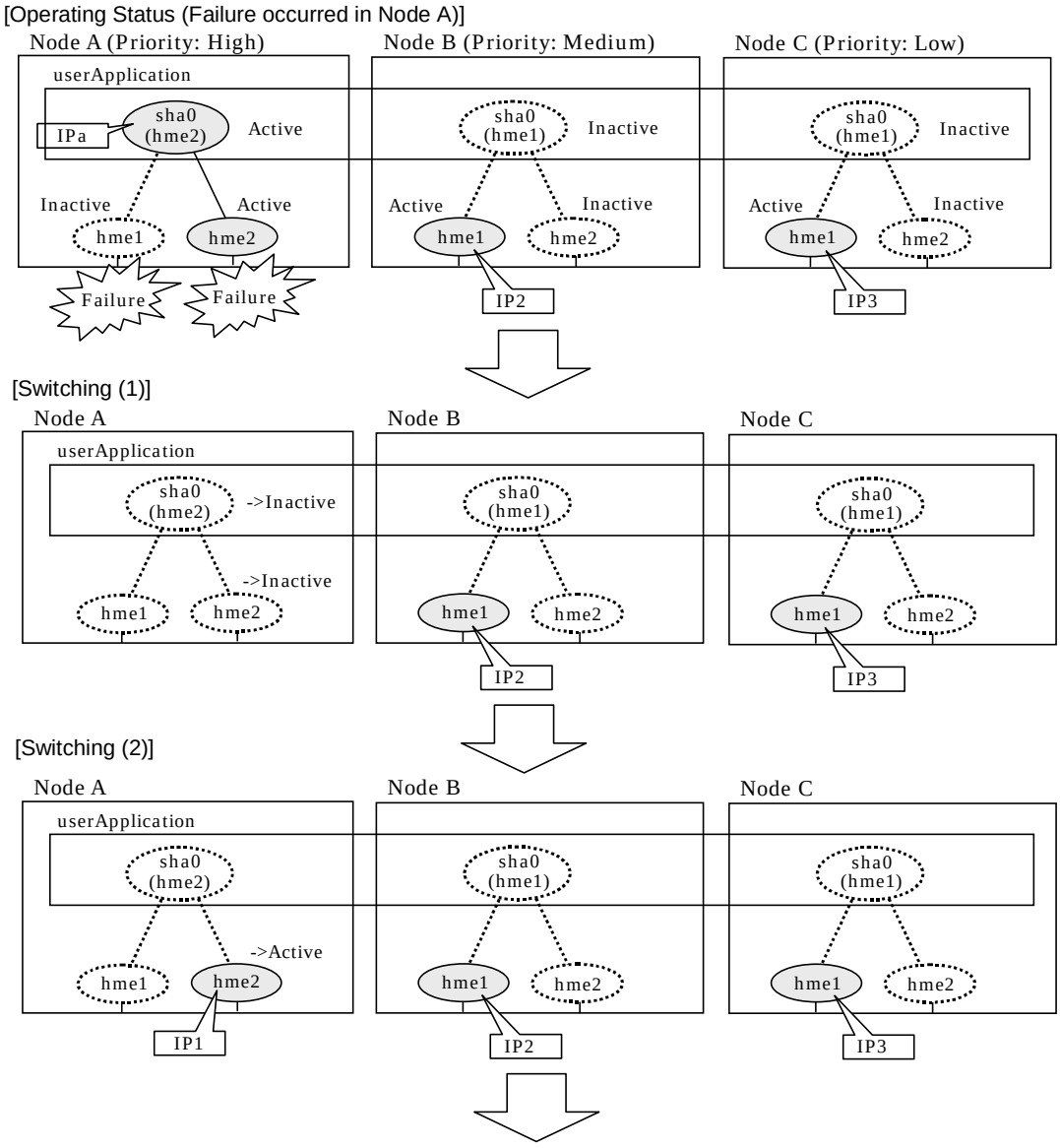
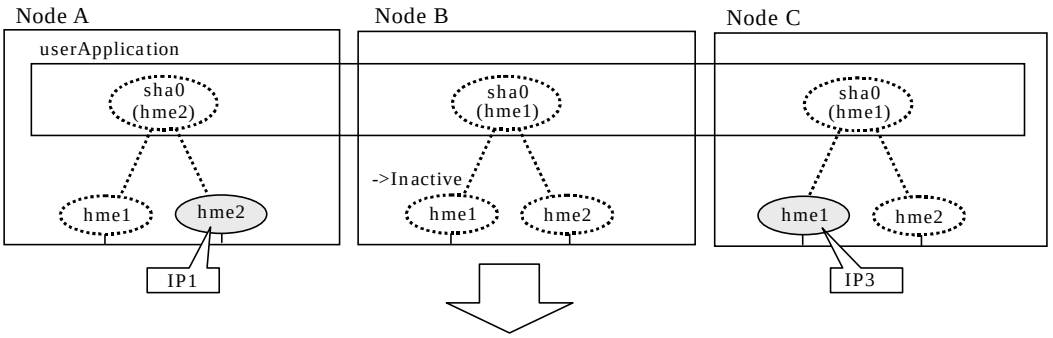


Figure 5.26 Switching operation of NIC switching mode (physical IP takeover I) (continues)

[Switching (3)]



[Finished switching]

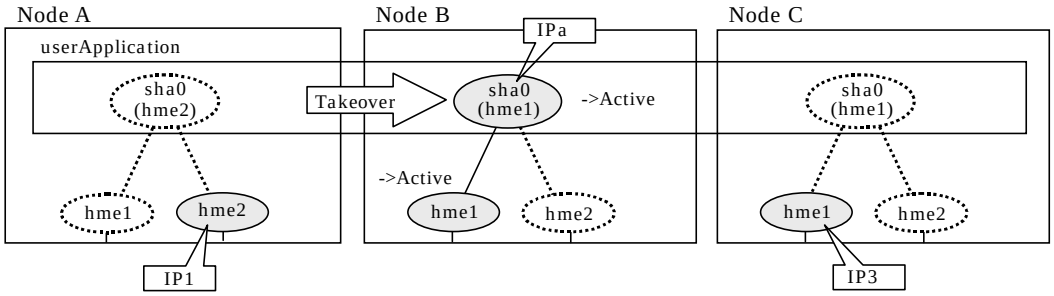


Figure 5.26 Switching operation of NIC switching mode (physical IP takeover I)

Figure 5.27 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 (hme1). After the IP address is successfully passed over to the standby node B, becomes inactive the secondary interface (hme2), which previously owned the takeover IP address (IPa) in node A.

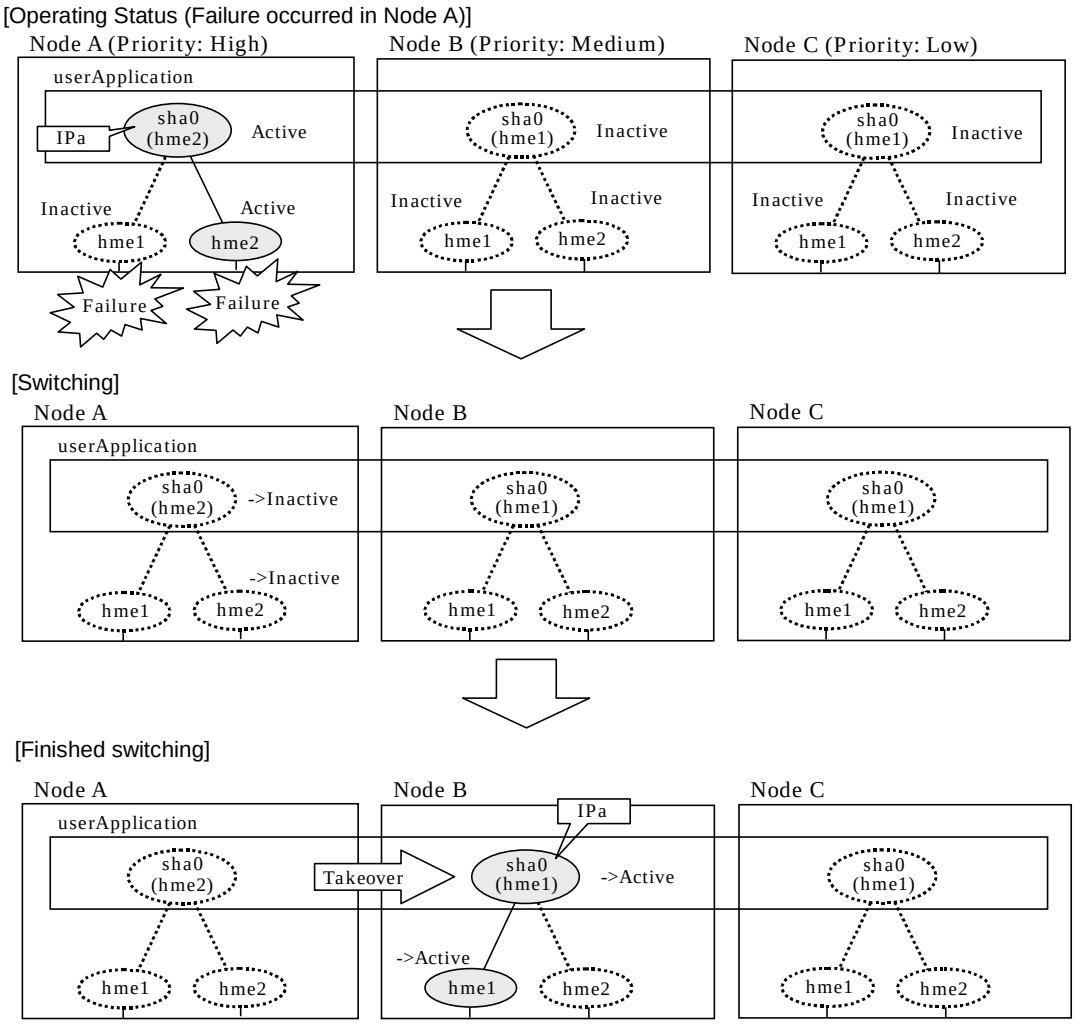


Figure 5.27 Switching operation of NIC switching mode (physical IP takeover II)

5.1.3.3 Fail-back

The following is a fail-back procedure, describing how to recover from the cluster switching.

1) Recovering the node, which encountered a failure

If switching was caused by panic or hang up, then reboot the node.
On the other hand, if switching was caused by a transfer path failure, then recover the transfer path encountered a failure. (Recovering options are reconnecting the cable, restore the power of HUB, and exchange the broken HUB.)

2) Fail-back to an arbitrary node on standby

Fails back a cluster application to an arbitrary node, which is on standby state.

5.1.3.4 Stopping

5.1.3.4.1 Fast switching mode

Figure 5.28 illustrates stopping operation of a userApplication

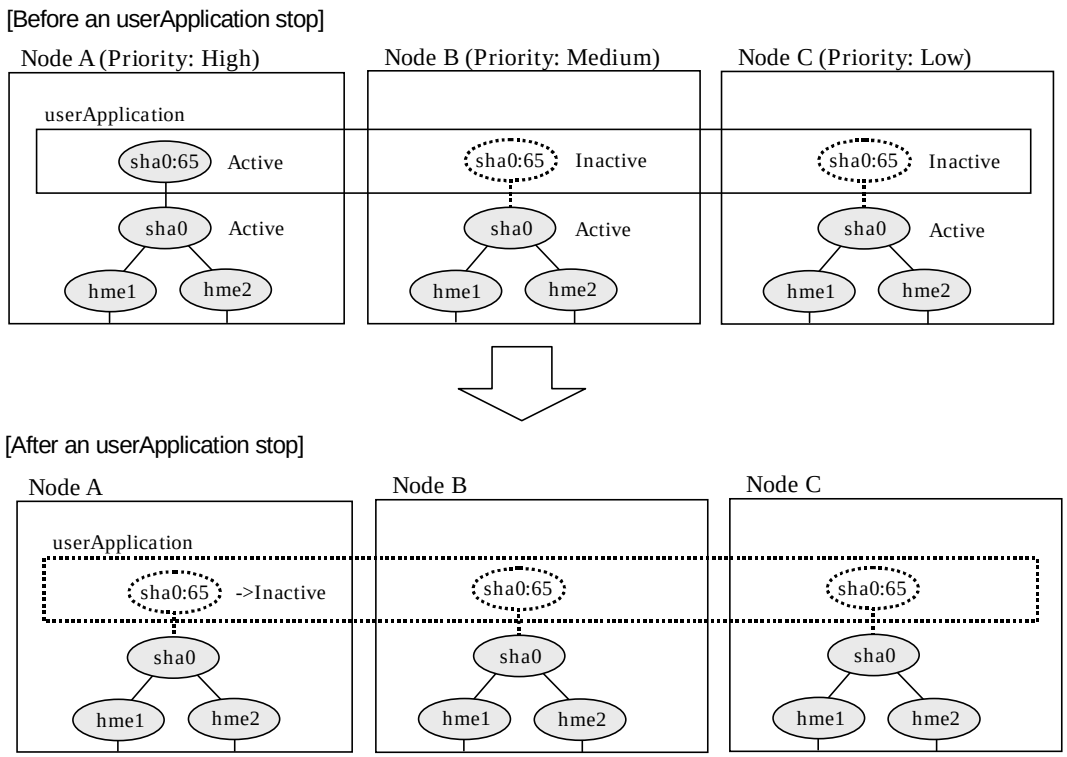


Figure 5.28 Stopping operation of Fast switching mode

5.1.3.4.2 NIC switching mode

Figure 5.29 illustrates stopping operation of a userApplication for logical IP takeover.

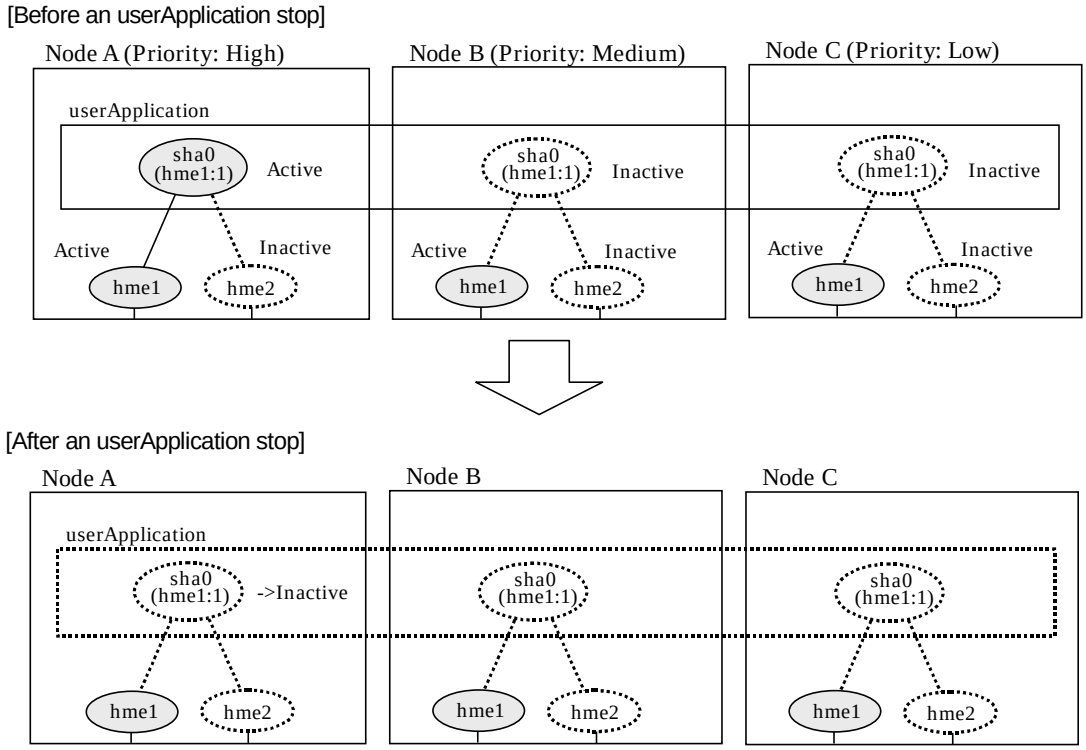


Figure 5.29 Stopping operation of NIC switching mode (logical IP takeover)

Figure 5.30 illustrates stopping operation of a userApplication for physical IP takeover I.

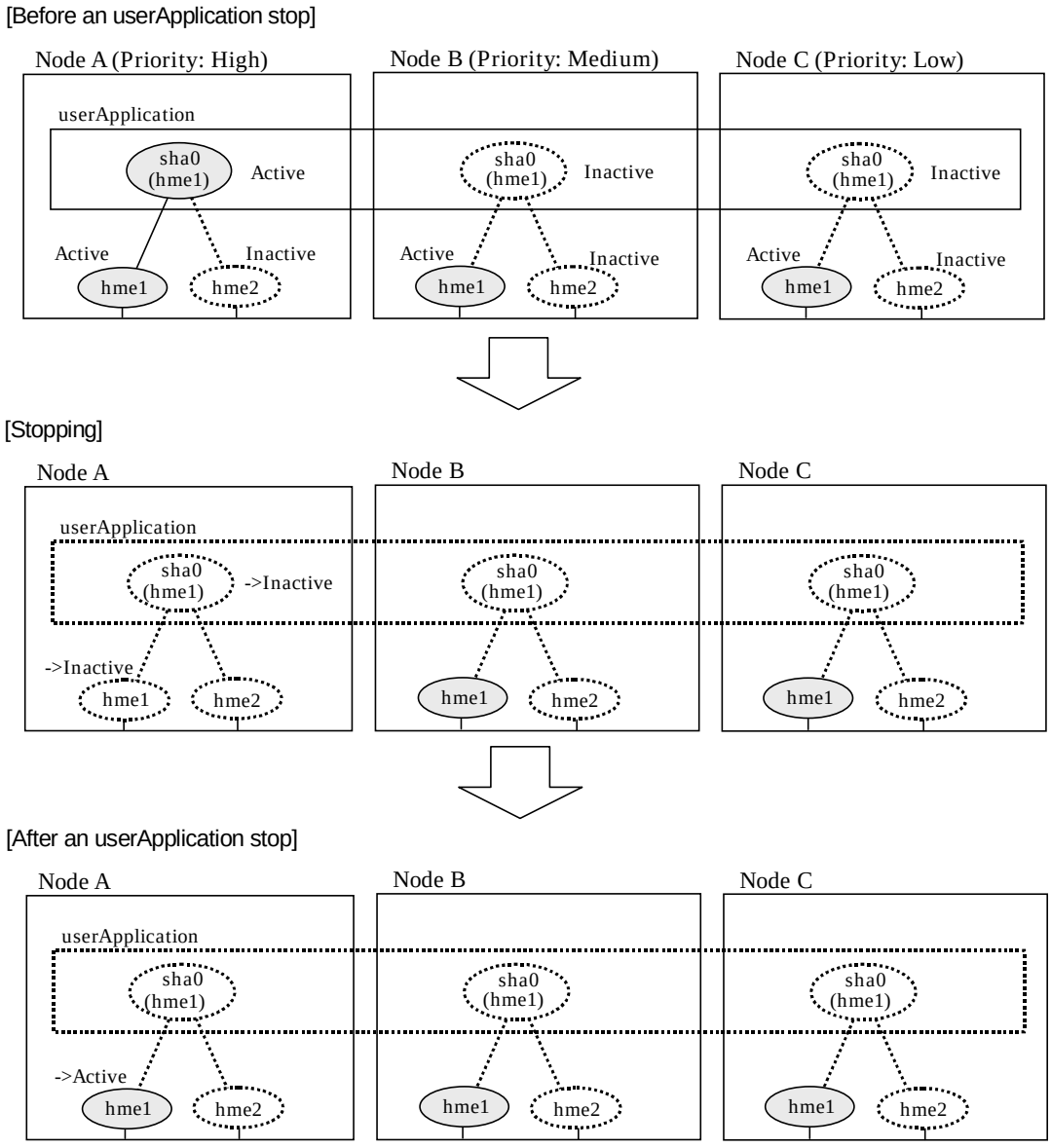


Figure 5.30 Stopping operation of NIC switching mode (physical IP takeover I)

Figure 5.31 illustrates stopping operation of a userApplication for physical IP takeover II.

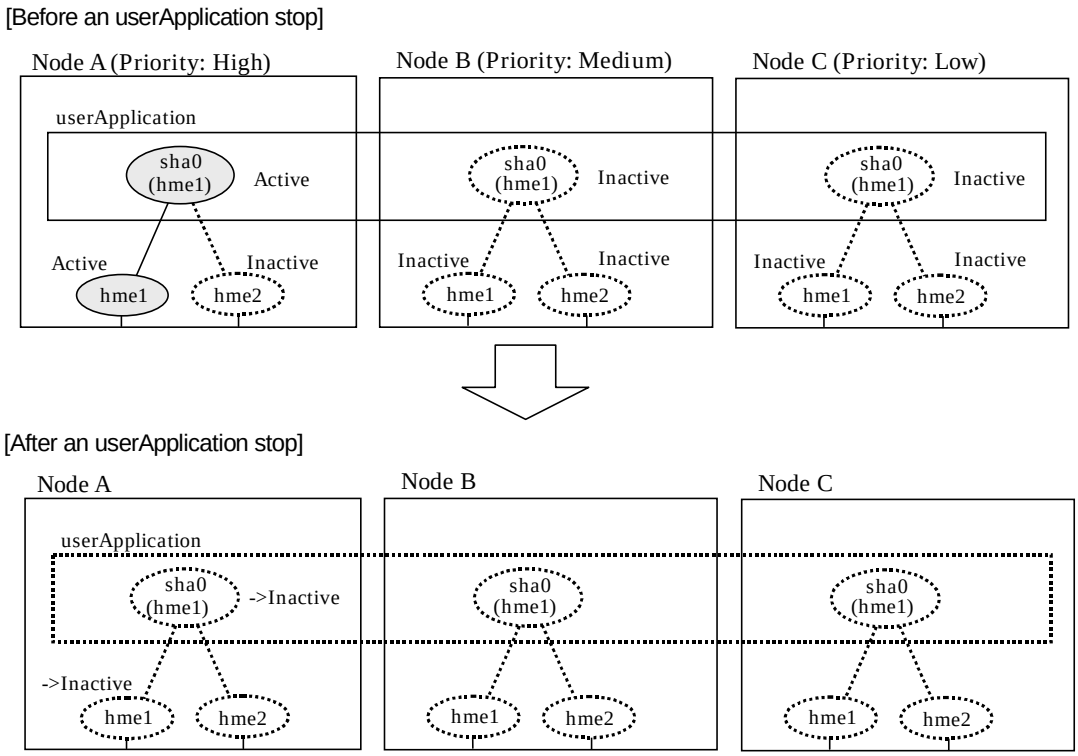


Figure 5.31 Stopping operation of NIC switching mode (physical IP takeover II)

5.1.4 Monitoring resource status of standby node

In a userApplication for standby operation, it is possible to monitor an operating node as well as a status of resource used in standby node of GLS.

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

5.1.4.1 Preface

Normally, a userApplication for standby operation does not monitor GLS resource status for standby node. In such case, even though a transfer path failure occurs in a standby node, the erroneous GLS resource remains to be unreleased and nothing is reported to the user. As a result, GLS resource error in standby node remains to be unsolved. To avoid this problem, GLS resource for standby node must be monitored with caution.

In order to monitor the GLS resource for a standby node, configure the “Standby Transition” when creating a userApplication.

Once the Standby Transition is successfully configured, it separates the erroneous GLS resource and reports the error to the user when a transfer failure occurs in a standby node. (This can be checked in “Cluster Admin” of Web-Based Admin View).

When using GS/SURE linkage mode on a cluster system, the virtual interface for standby side is inactive so that the standby side stops monitoring the remote system. Due to this, it cannot monitor GLS resources on the standby node. Therefore, it is not necessary to configure “StandbyTransition” attribute while creating userApplication in GS/SURE linkage mode.

5.1.4.2 Configuration

Refer to “6.6.2 Creating UserApplications” in “PRIMECLUSTER Installation and Administration Guide 4.1” for configuration of monitoring GLS resource status for a standby node.

5.1.4.3 Recovering from a resource failure in Standby node

See the following procedure for recovering GLS resource.

1) Recovering the transfer path failure

Restore the erroneous transfer path (Reconnecting the cable, restore the power of Switch/HUB, and replace the erroneous Switch/HUB)

2) Initializing GLS resource error

Clear the erroneous GLS resource status. (Use hvutil -c)
From this operation, GLS resource for standby node is reconfigured in a userApplication as a standby status.

5.1.5 Tagged VLAN interface multiplexing on NIC switching mode (Standby)

This section explains the transfer route multiplexing using tagged VLAN interface that operates on a cluster system.

5.1.5.1 Standby

5.1.5.1.1 Fast switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (standby).

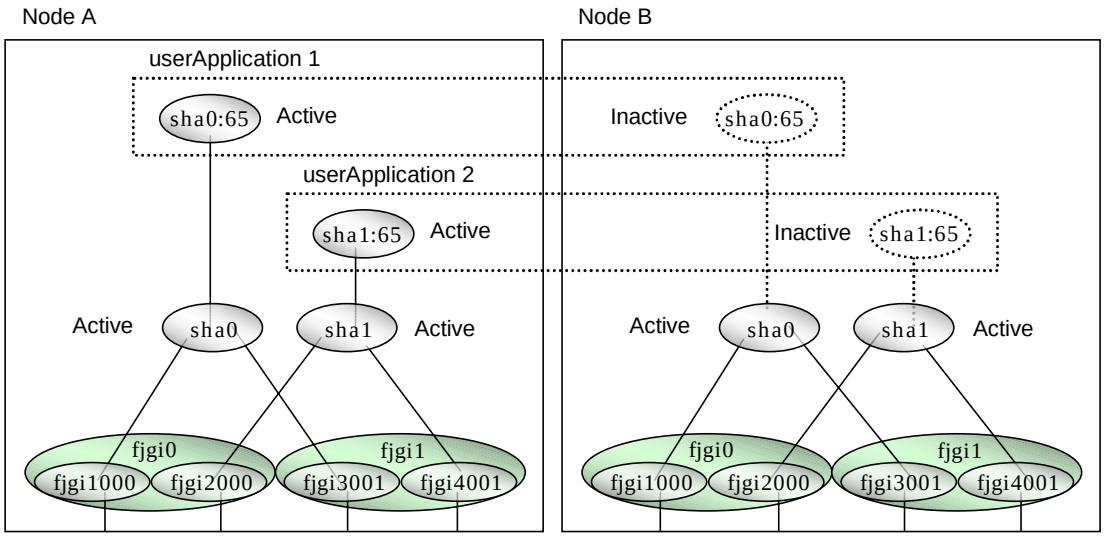


Figure 5.32 Tagged VLAN interface multiplexing on Fast switching mode (Standby)

5.1.5.1.2 NIC switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (standby).

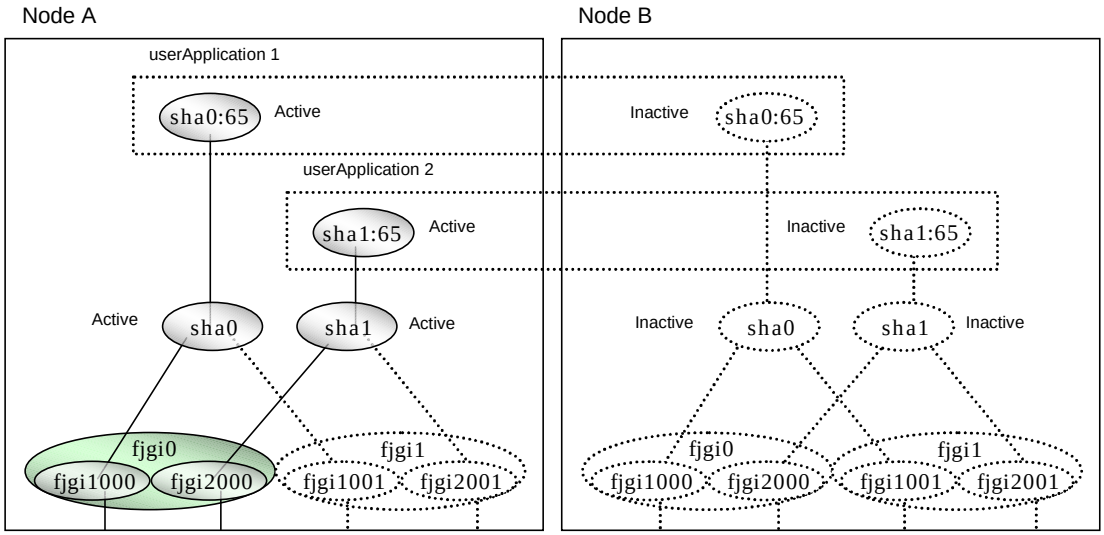


Figure 5.33 Tagged VLAN interface multiplexing on NIC switching mode (Standby)

5.1.5.2 Mutual Standby

5.1.5.2.1 Fast switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

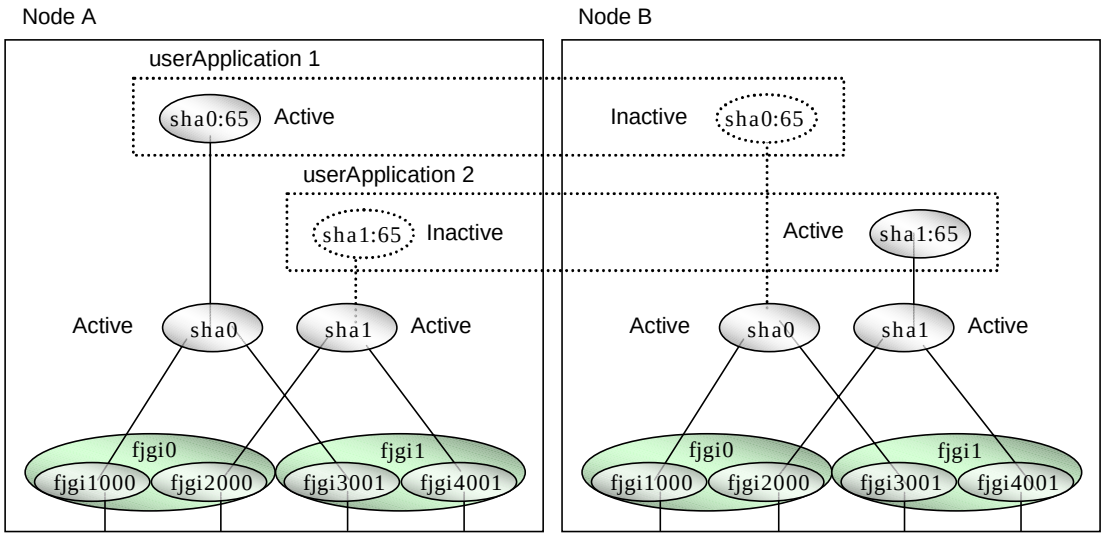


Figure 5.34 Tagged VLAN interface multiplexing on Fast switching mode (Mutual Standby)

5.1.5.2.2 NIC switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

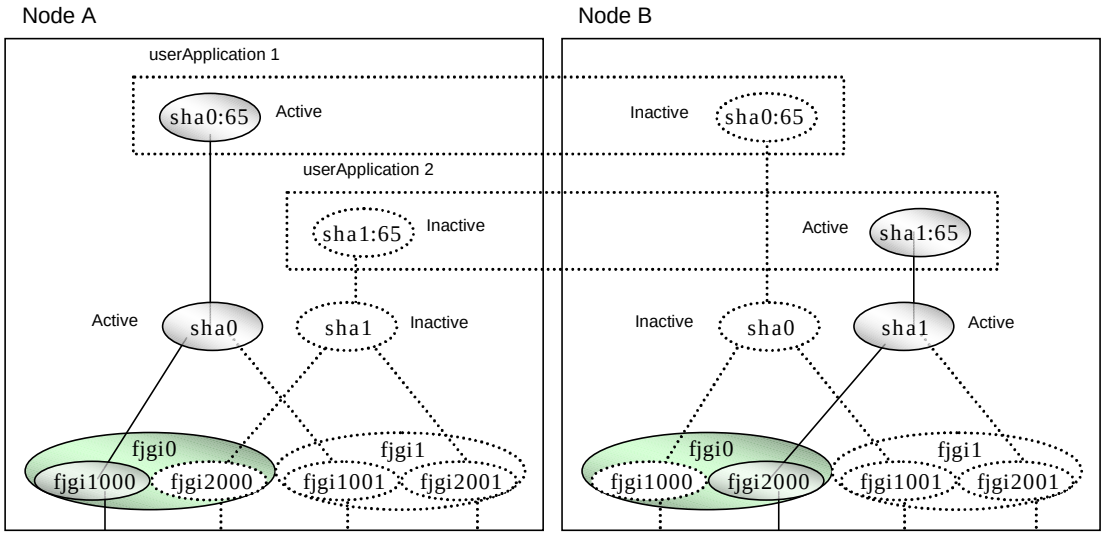


Figure 5.35 Tagged VLAN interface multiplexing on NIC switching mode (Mutual Standby)

5.1.5.3 Cascade

5.1.5.3.1 Fast switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

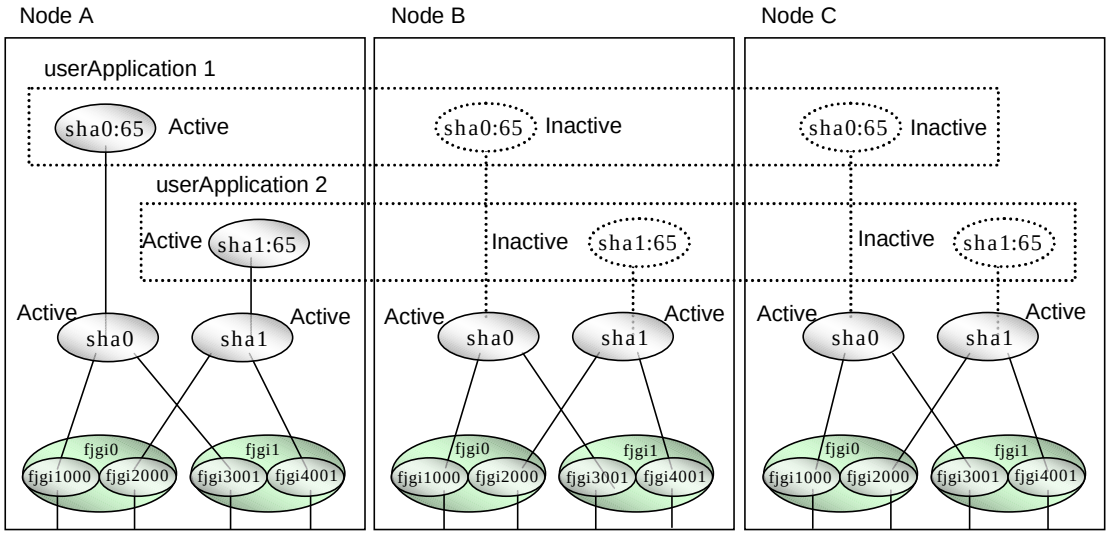


Figure 5.36 Tagged VLAN interface multiplexing on Fast switching mode (Cascade)

5.1.5.3.2 NIC switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

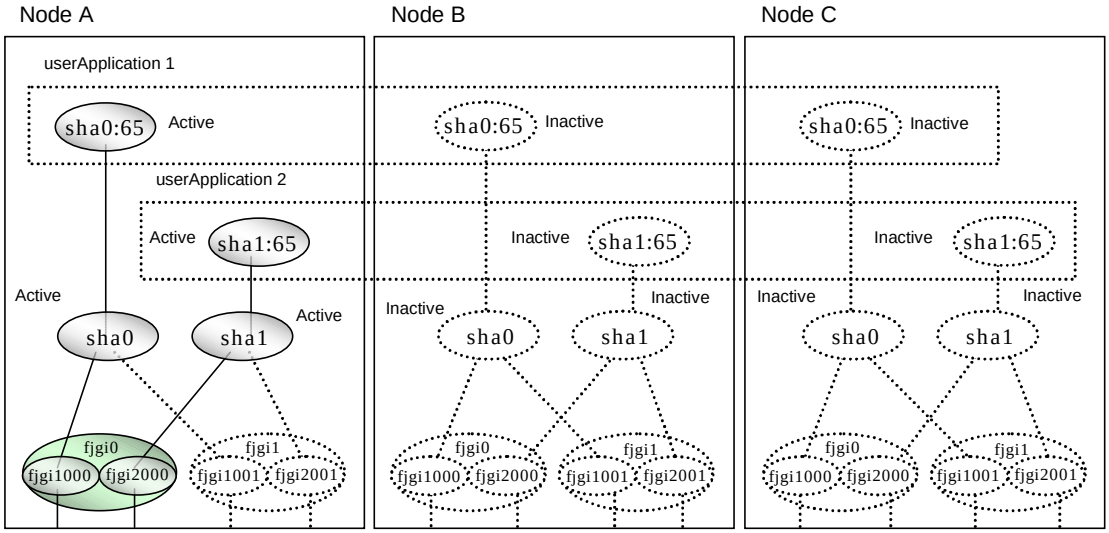


Figure 5.37 Tagged VLAN interface multiplexing on NIC switching mode (Cascade)

5.2 Adding configuration for Cluster System

In addition to configuring standard environment, configuration of takeover virtual interface and cluster environment is required for the cluster system.

Figure 5.38 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”.

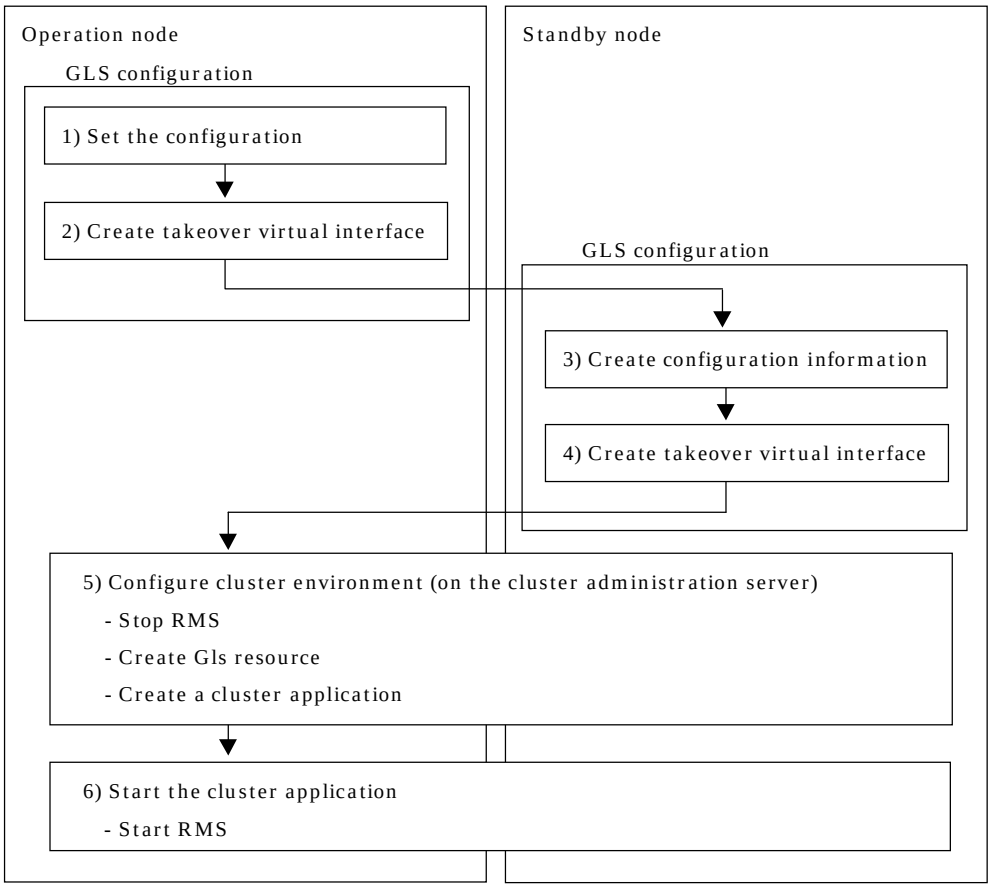


Figure 5.38 Flowchart for adding configuration for cluster system

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 lists the cluster definition operation commands.

Table 5.3 Cluster definition operation commands

Type	Command	Function	Authority
Registration/deletion/display of a virtual interface and the takeover resources.	/opt/FJSVhanet/usr/sbin/hanethvrsc	Registers/deletes/displays a virtual interface and the takeover resources.	Super user

5.2.1 Creating configuration information

Create the necessary configuration information for constructing a virtual interface. The information must be created on both the active and standby nodes. For details about the creation procedure, see “Chapter 3 Environment configuration".

5.2.2 Creating Takeover virtual interface

Takeover virtual interface for registering with userApplication is set up. It is necessary to perform this setup on all nodes. When setting for Fast switching mode, it is necessary to set a “takeover IP address”. (Not necessary to set for NIC switching mode.) An example of the setting is as follows. See “7.14 hanethvrsc Command” for the detail of the command.

If IPv6 address is used for the takeover virtual interface in Fast switching mode or NIC switching mode, it may take approximately 30 seconds to resume the connection after switching the node. However, by preliminary starting IPv6 routing daemon, the connection can be resumed immediately after switching the node. For details, refer to “D.2 Trouble shooting”.

[Configuring a takeover virtual interface]

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n “virtual-interface-name” [-i takeover-IP-address]
```

5.2.3 Configuring cluster system

Register the takeover virtual interface created in “5.2.2 Creating takeover virtual interface” as Gls resource, and create a userApplication. Cluster system can be configured using RMS Wizard. Refer to “PRIMECLUSTER Installation and Administration Guide 4.1” for details.

5.2.4 Starting a userApplication

After completing the configuration for a cluster system, start the userApplication.
Refer to “PRIMECLUSTER Installation and Administration Guide 4.1” for details.

5.3 Modifying configuration for Cluster System

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

5.4 Deleting configuration for Cluster System

For deleting the configuration of a cluster system, follow the figure below. For mutual standby operation, follow the steps from “2) Delete takeover virtual interface” up to “5) Delete configuration information” for the number of necessary nodes.

Note

Before deleting cluster configuration settings, it is recommended to backup the configuration settings of the cluster system. By preliminary backing up the configuration settings, it is possible to restore the system in case system trouble occurs and unable to recover from it. Refer to “5.5 Backup/Restore Cluster configuration settings” for details.

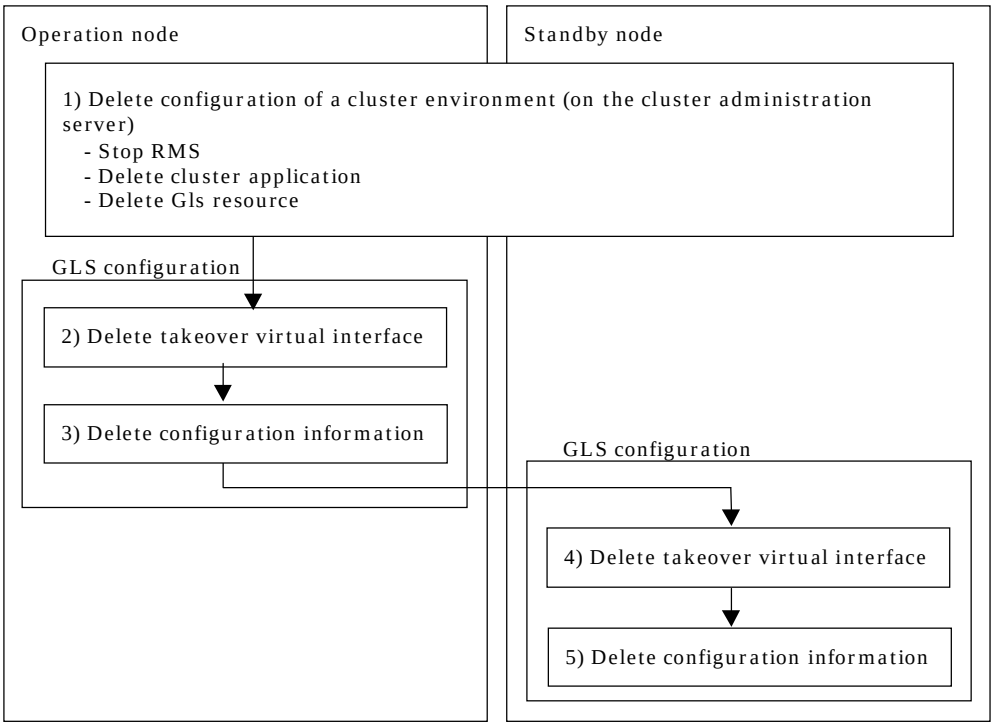


Figure 5.39 Flowchart for deleting configuration for cluster system

5.4.1 Deleting configuration for a cluster environment

Stop the RMS and delete the userApplication and Gls resource. Use RMS Wizard for this operation. Refer to “PRIMECLUSTER Installation and Administration Guide 4.1” for detail.

5.4.2 Deleting Takeover virtual interface

Delete a virtual interface to control a cluster from the resources database. It is necessary to perform this operation on all nodes.

An example of deletion is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n “logical-virtual-interface-name”
```

For detail, refer to "7.14 hanethvrsc Command".

5.4.3 Deletion of a Configuration information

Delete configuration information. Perform deletion process on the operating node and standby node. For deletion procedure, refer to “3.5 Deleting configuration information”.

5.5 Backup/Restore Cluster configuration settings

When operating Redundant Line Control function on a cluster system, it is possible to backup/restore the GLS configuration together with the cluster system configuration.

Redundant Line Control function is compliant with backing up/restoring the configuration settings of a cluster system. Executing the following commands enables backup/restore configuration settings of both cluster system and Redundant Line Control function.

```
Backup:
# /opt/SMAW/SMAWccbr/bin/cfbackup <Return>
Restore:
# /opt/SMAW/SMAWccbr/bin/cfrestore <Return>
```

For details on backing up and restoring the cluster system, refer to ”Chapter 11 Backing Up and Restoring a PRIMECLUSTER System” on “PRIMECLUSTER Installation and Administration Guide”.

Chapter 6 Maintenance

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

6.1 Redundant Line Control function Troubleshooting Data to be Collected

In the event of a problem in Redundant Line Control function operation, Redundant Line Control function troubleshooting requires following information about the problem to be collected. When collecting examination materials of a Redundant Line Control function all together, see "6.1.1 Command to collect materials".

1) Collecting materials common to each mode

Collect the following materials for examination when an error occurred in the workings of a Redundant Line Control function:

- The content of the detailed operation and error messages when a phenomenon occurred.
- A console log (/var/adm/messages) file
- A log file (/var/opt/FJSVhanet/log/*) of a Redundant Line Control function
- An environment setting file (/etc/opt/FJSVhanet/config/*) of a Redundant Line Control function
- The result of executing /opt/FJSVnet/usr/sbin/dsphanet
- The result of executing ifconfig -a
- The result of executing netstat -ni
- The result of executing netstat -nr
- The result of executing netstat -np

2) When an error occurred in Fast switching mode

When an error occurred in Fast switching mode, perform "1)Collecting materials common to each mode" and collect the following materials:

- The result of executing /opt/FJSVhanet/usr/sbin/dsphanet -o
- The result of outputting a driver trace of a Redundant Line Control function. (See "6.2 Trace" as to how to set, etc.)

3) When an error occurred in RIP switching mode

When an error occurred in RIP switching mode, perform "1) Collecting materials common to each mode" and collect the following materials:

- The result of executing ps -ef
- The result of executing /opt/FJSVhanet/usr/sbin/dsppoll (Only when using a router monitoring function.)

4) When an error occurred in Fast switching/RIP mode

When an error occurred in Fast switching/RIP mode, see "2) When an error occurred in Fast switching mode and 3) When an error occurred in RIP switching mode". Collect materials according to the operation state where an error occurred.

5) When an error occurred in NIC switching mode

When an error occurred in NIC switching mode, perform "1) Collecting materials common to each mode" and collect the following materials:

- The result of executing ps -ef
- The result of outputting a driver trace of a Redundant Line Control function when an error occurred in the workings of a using standby patrol function and in standby NIC. (See "6.2 Trace" as to how to set, etc.)

6) When an error occurred in GS/SURE linkage mode

When an error occurred in GS/SURE linkage mode, perform "1) Collecting materials common to each mode" and collect the following materials:

- The result of outputting a driver trace of a Redundant Line Control function. (See "6.2 Trace" as to how to collect, etc.)
- The result of executing /opt/FJSVhanet/usr/sbin/dsphanet -c
- The result of executing /opt/FJSVhanet/usr/sbin/dsppoll -c

6.1.1 Command to collect materials

[Form]

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

[Detail of the function]

This command collects examination materials necessary for maintaining a Redundant Line Control function.
In addition, only in the case of super-user authority, this command can be executed.

[Option]

It is possible to specify following options and parameters.

-s:

Specify -s to collect the minimum examination materials.
When omitted this opetion, all examination materials are collected.

save-directory:

Specify save-directory to store collected materials.
When omitted this parameter, materials are stored in "/tmp".

A list of the collected information is as follows:

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

Type	**File name when collected**	**Collected information**	**minimum examination materials**
System information: OSInfo/	etc/	/etc/hosts	Y
		/etc/netmasks	Y
		/etc/nsswitch.conf	Y
		/etc/gateways	Y
		/etc/hostname*	Y
		/etc/defaultrouter	Y
		/etc/notrouter	Y
	etc/inet	/etc/inet/*	Y
	etc/svc/log	/etc/svc/volatile/*	N
	etc/ipf	/etc/ipf/*	Y
	adm/	/var/adm/messages*	N
	var/svc/log	/var/svc/log/network-loopback:default.log	N
		/var/svc/log/network-physical:default.log	N
		/var/svc/log/network-initial:default.log	N
		/var/svc/log/network-service:default.log	N
		/var/svc/log/system-zones:default.log	N
		/var/svc/log/network-inetd:default.log	N

		/var/svc/log/network-fjsvhanet:default.log	N
		/var/svc/log/network-fjsvhanet-poll:default.log	N
	uname_a	uname -a	Y
	ifconfig_a	ifconfig -a	Y
	netstat	netstat -na netstat -ni netstat -np netstat -nr	Y
	filelist_etc	ls -l /etc/defaultrouter ls -l /etc/notrouter ls -l /etc/hostname*	Y
	ip_forward	/usr/sbin/ndd -get /dev/ip ip_forwarding	Y
	ipcs_a	ipcs -a	Y
	ipaddrsel	ipaddrsel	Y
	ipfstat	ipfstat -io	Y
	ps_ef	ps -ef	N
	pstack	pstack pid	N
GLS information: hanetInfo/	config/	/etc/opt/FJSVhanet/config/*	Y
	log/	/var/opt/FJSVhanet/log/*	Y
	version	hanetconfig version	Y
	patchinfo	patchadd -p | grep FJSVhanet	Y
	filelist_tmp	/var/opt/FJSVhanet/tmp/*	Y
	dsphanet	dsphanet dsphanet -o dsphanet -c	Y
	dsppoll	dsppoll dsppoll -c	Y
SafeCLUSTER information: SCInfo/	version_clapi	pkgparam FJSVclapi VERSION	N
	clgettree	clgettree	N
	clgettree_s	clgettree -s	N
PRIMECLUSTER information: RCInfo/	log/	/var/opt/reliant/log/*	N
	hvdisp_a	hvdisp -a	N

[Output form]

The collected materials are compressed and stored by tar and compress commands. A stored file name is "machine name" + "Date collected (YYMMDDhhmmss)".tar.Z.

Ex.) hostname031030084916.tar.Z

[Using example]

When collecting all examination materials under /tmp.

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

When collecting the minimum examination materials under /tmp.

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

When collecting the minimum examination materials under /export/home/user1.

```
# /opt/FJSVhanet/usr/sbin/hanet_snap -s /export/home/user1
```

6.2 Trace

This section explains how to collect driver trace for Redundant Line Control function.

6.2.1 Starting driver trace

[Synopsis]

/opt/FSUNnet/bin/strotr -k sha [-m msize] [-b bsize] [-a]

[Feature description]

Starts the collecting data of Redundant Line Control function trace logs.

[Options]

You can specify following options:

-k sha

Specifies the type of trace for drivers. Add "sha" to collect the trace for Redundant Line Control function.

-m msize

Specifies the buffer size in kilobytes for collecting the memory trace. The size has a range of 8 to 256 KB. The default value is 8 KB.

-b bsize

Specifies the maximum file size of the log file in kilobytes for collecting the file trace. The size has a range of 8 to 1,000 KB. The default value is 8 KB.
Since the trace data is collected in a log file, collecting a larger volume of file trace data than that of memory trace data is possible, but the result is a low processing speed.

-a

Specifies for collecting all of the data. The default assumes that 64 bytes of the data should be collected.

[Related commands]

stpotr
prtotr

[Notes]

If both -m option and -b option are not specified, the driver trace is performed as a memory trace.
If both -m option and -b option are specified, the processing of the file trace has a higher priority.

[Example]

- The following is an example of collecting the memory trace (when all of the data is to be collected with the trace buffer size for the main memory specified as 256 KB):

```
# strotr -k sha -m 256 -a
```

- The following is an example for collecting the file trace (when the maximum size of the log file is specified as 1,000 KB and collecting all of the data is not necessary):

```
# strotr -k sha -b 1000
```

6.2.2 Stopping driver trace

[Synopsis]

/opt/FSUNnet/bin/stpotr -k sha

[Feature description]

Stops collecting Redundant Line Control function trace logging data.

[Option]

You can specify following option:

-k sha

Specifies the type of trace for drivers. Specify the same "sha" (trace type) specified at the start of trace collection.

[Related commands]

strotr
prtotr

[Examples]

- The following is an example of stopping the driver trace:

```
# stpotr -k sha
```

6.2.3 Outputting driver trace

[Synopsis]

/opt/FSUNnet/bin/prtotr -k sha

[Feature description]

Outputs the collected Redundant Line Control function trace logging data.

[Option]

You can specify following option:

-k sha

Specifies the type of trace for drivers. Specify the same "sha" (trace type) specified at the start of trace collection. If this option is not specified, all collected traces currently in memory are displayed.

[Related commands]

strotr
stpotr

[Examples]

- The following is an example of outputting the driver trace:

```
# prtotr -k sha
```

6.2.4 Precautions about driver trace function

An operator with the superuser privilege can execute the strotr, stpotr or prtotr commands.

Since the high load on the CPU under trace processing deteriorates performance, trace should be performed sparingly.

A log file is created in the /var/opt/FJSVhanet/otr directory. When specifying the maximum size for the log file with the -b option, be sure to check for available disk space beforehand.

Collecting trace data by running a file trace may lead to a loss of trace data, but this event is rare.

If an invalid option is specified in a command (strotr, stpotr and prtotr commands), only commands with valid options are processed, and commands with invalid options are ignored.

Notes on collecting a driver trace:

A driver trace overwrites the old information because not possible to collect the information exceeding the specified buffer size or memory size. Therefore, clarify the procedure of the occurrence of a phenomenon, and make the time to activate a driver trace as short as possible. The procedure to collect a driver trace is as follows:

1) To start a driver trace of a Redundant Line Control function

```
# /opt/FSUNnet/bin/strotr -k sha -m 256 -A
```

2) To execute the procedure of reproduction

```
(The procedure of reproduction)
```

3) To stop a driver trace of a Redundant Line Control function

```
# /opt/FSUNnet/bin/stpotr -k sha
```

4) To output a driver trace of a Redundant Line Control function

In the following example, the result of outputting is output to a /tmp/sha.otr file.

```
# /opt/FSUNnet/bin/prtotr -k sha > /tmp/sha.otr
```

When collecting a driver trace in file trace mode, stop unnecessary communication on a transfer route. When there are many pieces of the collecting information, occasionally not possible to trace.

Chapter 7 Command reference

This chapter outlines GLS commands.

7.1 hanetconfig Command

[Name]

hanetconfig - Setting, modifying, deleting, and displaying a configuration definition of Redundant Line Control function

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetconfig command [args]

[Feature description]

The hanetconfig command defines configuration information required for the operation of Redundant Line Control function. This command also modifies, deletes, and displays a setting.

Command	Process outline	Authority
create	Creates configuration information	Super user
copy	Copies configuration information	Super user
print	Displays configuration information	General user
modify	Modifies configuration information	Super user
delete	Deletes configuration information	Super user
version	Displays the version	General user

(1) create command

Configuration information must be defined for a virtual interface before Redundant Line Control function can be operated. Use the create command to create a definition of configuration information. The create command can also create definitions of more than one logical virtual interface on the virtual interface. The following is the command format for building a virtual interface:

- When creating a virtual interface

Fast switching mode (IPv4):
/opt/FJSVhanet/usr/sbin/hanetconfig create [inet] -n devicename -m t -i ipaddress -t interface1[,interface2,...]

Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n devicename -m t -t interface1[,interface2,...]

RIP mode or Fast switching/RIP mode:
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m {r | b} -i ipaddress -t interface1[,interface2,...]

GS/SURE linkage mode (physical interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m n -i ipaddress -t interface

GS/SURE linkage mode (virtual interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m c -i ipaddress -t 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 failback if a failure occurs / immediate automatic failback):
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m {p | q} -a MAC_address -t interface

- When creating a logical virtual interface

Fast switching mode, RIP mode and Fast switching/RIP mode (IPv4):
/opt/FJSVhanet/usr/sbin/hanetconfig create [inet] -n devicename -i ipaddress

Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n devicename -i ipaddress/prefix

[inet | inet6]

Specify an IP address form to set to a virtual interface.

inet : IPv4 address
inet6 : IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of "create") before other options.
This option can be specified only when using Fast switching mode or NIC switching mode (a logical IP address takeover function).

-n devicename:

Specify the name of a virtual interface or logical virtual interface for which the configuration information should be set. Specify the virtual interface name with a string that begins with "sha" and is followed by a value (0 to 255) (such as sha0 and sha10). Specify the logical virtual interface name as "virtual-interface-name: value (2 to 64)" (such as sha0:2 and sha10:5). If you specify a virtual interface or logical virtual interface in any other format, an error message is output and this command terminates abnormally. In addition, Logical virtual interface can only be configured on operation mode "t".

-m t|r|b|n|c|d|e|p|q:

Specify an operation mode. If devicename is a logical virtual interface, specify the operation mode of a corresponding virtual interface.

t: Fast switching mode
Specify this parameter to use the Redundant Line Control function in Fast switching mode.

r: RIP mode
Specify this parameter to use the Redundant Line Control function in RIP mode.

b: Fast switching/RIP mode
Specify this parameter to use the Redundant Line Control function in Fast switching/RIP mode.

n: GS/SURE linkage mode (physical interface definition)
Specify this parameter to use the Redundant Line Control function in GS/SURE linkage mode. A physical interface used to actually perform communication is created.

c: GS/SURE linkage mode (virtual interface definition)
Specify this parameter to use the Redundant Line Control function in GS/SURE linkage mode. A virtual interface that bundles physical interfaces defined in operation mode n to perform communication is created.

d: NIC switching mode (logical IP address takeover function)
Specify this parameter to use the Redundant Line Control function in NIC switching mode. This mode activates logical interface and physical interface.

e: NIC switching mode (physical IP address takeover function)
Specify this parameter to use the Redundant Line Control function in NIC switching mode. This mode activates only physical interface.

p: Standby patrol function (automatic failback if a failure occurs)
Specify this parameter to use the Redundant Line Control function in NIC switching mode and monitor the status of the standby NIC. If the standby NIC is communicating due to a failure and the active NIC recovers, no failback occurs until the currently used NIC encounters a failure.

q: Standby patrol function (immediate automatic failback)
Specify this parameter to use the Redundant Line Control function in NIC switching mode and monitor the status of the standby NIC. If the standby NIC is communicating due to a failure and the active NIC recovers, a failback immediately occurs.

The following table lists options that can be specified in each operation mode.

Specifiable parameter / Operation mode	**inet | inet6**	**-n**	**-i**	**-e**	**-a**	**-t**
‘t’ (Fast switching mode)	Support	O	O (*8)	X	X	O (*1)
‘r’ (RIP mode)	Not support	O	O	X	X	O (*1)
‘b’ (Fast switching/RIP mode)	Not support	O	O	X	X	O (*1)
‘n’ (GS/SURE linkage mode (physical interface definition))	Not support	O	O	X	X	O (*2)
‘c’ (GS/SURE linkage mode (virtual interface definition))	Not support	O	O	X	X	O (*3)
‘d’ (NIC switching mode (logical IP address takeover function))	Support	O	O	O (*6)	X	O (*4)
‘e’ (NIC switching mode (physical IP address takeover function))	Not support	O	O	O (*7)	X	O (*4)
‘p’ (Standby patrol function (automatic failback if a failure occurs))	Not support	O	X	X	O	O (*5)
‘q’ (Standby patrol function (immediate automatic failback))	Not support	O	X	X	O	O (*5)

[Meaning of the symbols] 0: Required, X: Not required

*1 Specify a physical interface (The same physical interface can be specified if the operation mode is "t", "r", or "b"). 1 to 8 physical interfaces can be assigned.
*2 Specify one physical interface that is not specified in any other operation mode. Only one physical interface can be assigned.
*3 Specify a virtual interface created in operation mode "n". Two interfaces can be assigned.
*4 Specify a physical interface that is not specified in any other operation mode. One or two physical interface can be assigned.
*5 Specify a virtual interface specified in the operation mode "d" or "e". Only one

interface can be assigned.
*6 It is not possible to specify this parameter when set inet6 to an address form.
*7 This parameter may be omitted if the physical IP address takeover function II is used (not activating an interface on the standby node in the cluster system).
*8 It can specify, only when creating logical virtual interface.

-i ipaddress1[/prefix]:

ipaddress1

Specify a host name or an IP address to assign to a virtual interface or a logical virtual interface (devicename specified by -n option). The specified IP address or host must be defined in an /etc/inet/hosts file (IPv4) or an /etc/inet/ipnodes file (IPv4,IPv6). When assigning an IP address to a logical virtual interface, it is necessary to specify the same subnet as that of a virtual interface. If specified a different subnet, occasionally it is not possible to communicate.

[/prefix]

Specify the length of a prefix of ipaddress1 following "/" (slash). The range possible to specify is between zero to 128. This parameter is required only when specifying an IPv6 address to ipaddress1 or a host name defined in an /etc/inet/ipnodes file. It is not possible to specify for an IPv4 address.

-e ipaddress2:

Specify an IP address or a host name to assign to a physical interface. It is possible to set an IP address or a host name in an IPv4 form only and must be defined in an /etc/inet/hosts and /etc/inet/ipnodes files. It is possible to specify this option only when specified inet for an address form. (When specified inet6, a link local address is automatically assigned.) It is necessary to set this option in NIC switching mode (operation mode is "d" or "e"). 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 GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

To configure other than GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"), specify the name of physical interface (such as eri0 or hme0) or the name of tagged VLAN interface (such as ce1000 or fjgi1000).

-a MAC_address:

Specify a local MAC address to be allocated to the standby NIC as 02:XX:XX:XX:XX:XX (X represents a hexadecimal from 0 to F). "02" in the beginning indicates that this is a local MAC address. Any value may be specified. However, manage the address to prevent duplication of addresses with other NICs connected on the same LAN. No normal operation is guaranteed if duplicate addresses are used.

This parameter must be set only if the standby patrol function (operation mode "p" or "q") is used.

(2) copy command

Use the copy command to create different configuration information while sharing an NIC used in other configuration information (virtual interface in NIC switching mode (operation mode "d")). This command thus allows configuration information to be automatically created by using the copy source information and without requiring you to specify an IP address to be attached to a physical interface, interface names to be bundled by a virtual interface, and an operation mode. This command realizes simpler operation than directly executing the hanetconfig create command.
In addition, this command can copy only virtual interface of NIC switching mode (operation mode "d").

The following is the command format for copying a virtual interface:

- When duplicating a virtual interface of IPv4 from a virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy [inet] -n devicename1,devicename2 -i
ipaddress
```

- When duplicating a virtual interface of IPv4 from a virtual interface of IPv6 (dual stack configuration)

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy [inet] -n devicename1,devicename1 -i
ipaddress1 -e ipaddress2
```

- When duplicating a virtual interface of IPv6 from a virtual interface of IPv6

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n devicename1,devicename2 -i
ipaddress/prefix
```

- When duplicating a virtual interface of IPv6 from a virtual interface of IPv4 (dual stack configuration)

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n devicename1,devicename1 -i
ipaddress/prefix
```

[inet | inet6]

Specify an IP address form to set to a copy-to virtual interface.

inet : IPv4 address
inet6 : IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a strings of copy) before other options.

-n devicename1,devicename2:

devicename1:

Specify a copy-from virtual interface name. It is possible to specify only a virtual interface name of NIC switching mode (operation mode is "d").

devicename2:

Specify a copy-to virtual interface name. When configuring IPv4/IPv6 dual stack, specify the same virtual interface name (devicename1) as that of copy-from.

-i ipaddress1[/prefix]:

Specify a host name or an IP address to assign to a copy-to virtual interface specified by devicename2. See -i option of a create command for the detail of how to set.

-e ipaddress2:

Specify an IP address or a host name to assign to a physical interface. This option is required to duplicate a virtual interface of IPv4 from that of IPv6 (dual stack configuration). See -e option of a create command for the detail of how to set.

(3) print command

Use the print command to display the current configuration information. The following is the format of the print command.

```
/opt/FJSVhanet/usr/sbin/hanetconfig print [-n devicename1[,devicename2,...]]
```

-n devicename1[,devicename2,...]:

Specify the name of a virtual interface or logical virtual interface whose configuration information

should be displayed. If this option is not specified, the print command displays all the configuration information for the currently set virtual interfaces and logical virtual interfaces.

The following shows an example of displaying configuration information.

```
[IPv4,Patrol]

 Name        Hostname        Mode MAC Adder/Phys ip Interface List
+-----------+---------------+----+-----------------+------------------+
 sha0        hostA            t                     hme0,hme1
 sha1        10.0.1.1         r                     hme0,hme1
 sha12       -                p   02:00:00:00:00:01 sha11
 sha2        hostC            d                     fjgi1000,fjgi1001
 sha3        -                p   02:00:00:00:00:10 sha2

[IPv6]

 Name        Hostname/prefix                   Mode Interface List
+-----------+---------------------------------+----+------------------+
 sha10       -                                  t   qfe0,qfe1
 sha10:2     hostB/64
 sha11       fec0:1::123/64                     d   qfe2,qfe3
```

Item		Explanation
[IPv4,Patrol]		The information of an IPv4 virtual interface and standby patrol
[IPv4,Patrol]	Name	Outputs a virtual interface name.
	Hostname	Outputs the host name or virtual IP address of a virtual interface.
	Mode	Outputs the operation mode of a virtual interface. (For details, please refer to "-m" option of the create command.)
	MAC Adder/Phys ip	Outputs a MAC local address used by standby patrol mode, or physical IP address defined as the virtual interface.
	Interface List	Outputs a virtual interface name in GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"). Outputs a physical interface name (such as le0 and hme0) in any other mode than GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").
[IPv6]		The information of an IPv6 virtual interface
[IPv6]	Name	Outputs a virtual interface name.
	Hostname/prefix	A host name or an IP address and a prefix value of a virtual interface
	Mode	Outputs the operation mode of a virtual interface.
	Interface List	Outputs a virtual interface name in GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"). Outputs a physical interface name (such as le0 and hme0) in any other mode than GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

(4) modify command

Use the modify command to modify the configuration of Redundant Line Control function.
The following is the format of the modify command that modifies configuration information for a virtual interface:

- When changing configuration information of a virtual interface

Fast switching mode (IPv4):
/opt/FJSVhanet/usr/sbin/hanetconfig modify [inet] -n devicename {[-m {r | b}] [-i ipaddress1] [-t interface1[,interface2,...]]}

Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig modify inet6 -n devicename -t interface1[,interface2,...]

RIP mode or Fast switching/RIP mode:
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[-m {t | r | b}] [-i ipaddress] [-t interface1[,interface2,...]]}

GS/SURE linkage mode (physical interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[-i ipaddress] [-t interface]}

GS/SURE linkage mode (virtual interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[-i ipaddress] [-t interface1[,interface2,...]]}

NIC switching mode (IPv4: logical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig modify [inet] -n devicename {[-i ipaddress1] [-e ipaddress2] [-t interface1[,interface2]]}

NIC switching mode (IPv6: logical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig modify inet6 -n devicename {[-i ipaddress1/prefix] [-t interface1[,interface2]]}

NIC switching mode (physical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[-i ipaddress1] [-e ipaddress2] [-t interface1[,interface2]]}

Standby patrol function:
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[-a MAC_Address] [-t interface1]}

- When changing configuration information of a virtual interface

Fast switching mode, RIP mode and Fast switching/RIP mode (IPv4):
/opt/FJSVhanet/usr/sbin/hanetconfig modify [inet] -n devicename -i ipaddress

Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig modify inet6 -n devicename -i ipaddress/prefix

[inet | inet6]

Specify an IP address form to set to a changing virtual interface.

inet	: IPv4 address
inet6	: IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of modify) before other options.
This option can be specified only when using Fast switching mode or NIC switching mode (a logical IP address takeover function).

-n devicename:

Specify the name of a virtual interface or logical virtual interface whose configuration information should be modified. This parameter is required.

-m t|r|b:

Specify this parameter to change the operation mode (Fast switching mode, RIP mode, or Fast switching/RIP mode) of a virtual interface to be modified. One of Fast switching mode, RIP mode, or Fast switching/RIP mode can be selected (“t” indicates Fast switching mode, “r” indicates RIP mode, and “b” indicates Fast switching/RIP mode).

-i ipaddress1[/prefix]:

Specify a host name or IP address to be attached to a virtual or logical virtual interface (devicename specified by -n option) to be used for Redundant Line Control function. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts and /etc/inet/ipnodes files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation. When you specify address information for a logical virtual interface, be sure to specify an address in the same subnet as the address of a corresponding virtual interface. Communication may be disabled if any other subnet is specified.

-e ipaddress2:

Specify an IP address to be attached to a physical interface. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts and /etc/inet/ipnodes files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation.

This parameter can be modified only if the operation mode of a virtual interface to be modified is NIC switching mode (operation mode "d" or "e").

-t interface1[,interface2,...]:

Specify interface names to be bundled by a virtual interface, by listing them delimited with a comma (,).

Specify virtual interface names (such as sha1 and sha2) if the operation mode of a virtual interface to be modified is GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

Specify physical interface names (such as le0 and hme0) if the operation mode of a virtual interface to be modified is not GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

-a MAC_address:

This parameter can be changed only if the operation mode of a virtual interface to be modified is standby patrol function (operation mode "p" or "q").

(5) delete command

Use the delete command to delete the configuration of Redundant Line Control function. The following is the format of the delete command:

```
/opt/FJSVhanet/usr/sbin/hanetconfig delete [inet | inet6] -n
{devicename1[,devicename2,...] | all}
```

[inet | inet6]

Specify an IP address form of a deleting virtual interface.

inet	: IPv4 address
inet6	: IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of delete) before other options.
This option can be specified only when using Fast switching mode or NIC switching mode (a logical IP address takeover function).

-n devicename1[,devicename2,...]:

Specify the names of virtual interfaces (such as sha0 and sha1) or logical virtual interfaces (such as sha0:2 and sha1:10) whose configuration information should be deleted.

all:

Specify this parameter to delete all the defined virtual and logical interfaces. In addition, the definition of IPv4 interface and IPv6 interface cannot be deleted simultaneously. Please specify IPv4 interface and IPv6 interface individually, respectively and delete them.

(6) version command

The version of this product is displayed. The following is the format of the version command.

```
/opt/FJSVhanet/usr/sbin/hanetconfig version
```

The following shows an example of displaying version information.

```
HA-Net version 2.7
```

[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 router/HUB monitoring is set, no relevant configuration information can be deleted. Delete configuration information after deleting the relevant information of the router/HUB monitoring function.
- A physical interface to be specified for GS/SURE linkage mode (operation mode "n") must not be defined for the use in conventional TCP/IP. (Check if or not there is /etc/hostname.interface file. If exists, change a name or delete it, then execute "/usr/sbin/ifconfig interface unplumb" command.)
- An IP address or host name to be specified to create, copy, or modify configuration information must be defined in /etc/inet/hosts and /etc/inet/ipnodes.
- If more than one virtual interface is created while sharing a NIC bundled in NIC switching mode, the standby patrol need not be set for each of the virtual interfaces.
- When specified a numeric string for a host name, it is dealt with as decimal and converted into an IP address corresponding to its value to work. (For instance, when specified "123456", it is regarded an IP address "0.1.226.64" is specified.)
- As for an actual interface to configure Fast switching mode, RIP mode, and Fast switching/RIP mode (the operation mode is "t", "r", and "b"), be sure to define to use in TCP/IP before defining a virtual interface. (Check if or not there is /etc/hostname.interface file. If not, create it and reboot a system.)
- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change the corresponding host name on the host database of such as /etc/inet/hosts and /etc/inet/ipnodes files. To change the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.
- When using an IPv6 address, an IP address that is set by -i option of a create command is not a target of address automatic configuration by an IPv6 protocol. Therefore, specify the same to a prefix and the length of a prefix as those set in an IPv6 router on the connected network. Set a value different from that of the other system for an "interface IP" inside an IP address field.
- When configuring a virtual interface for Fast switching mode as Dual Stack, the bundled physical interfaces cannot be modified with “modify –t” command. To apply changes, delete the configuration information of the virtual interface and then reconfigure.

- Do not use characters other than alphanumeric characters, period, and hyphen for the host name. If characters other than the above are used, re-write the host names in /etc/inet/hosts and /etc/inet/ipnodes so that it does not contain any other characters. Also, the first and last character for the host name must be alphanumeric character.
- When configuring a standby patrol function for a virtual interface which is using the tagged VLAN interfaces, it is required to reboot the OS in order to enable the standby patrol function. GLS withholds a modification of MAC address of the secondary interface, so that it prevents communication errors on other tagged VLAN interfaces which are sharing a physical communication line.

[Examples]

(1) create command

The following shows an example of the setting command used in Fast switching mode to bundle two physical interfaces (hme0 and hme1) as the virtual interface host “hahost” to duplicate the virtual interface sha0.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i hahost -t hme0,hme1
```

The following shows an example of the setting command used in RIP mode to have each of two virtual interfaces (sha0 and sha1) bundle two of four physical interfaces (hme0, hme1, hme2, and hme3).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i hosta -t hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m r -i hostb -t hme2,hme3
```

The following shows an example of the setting command used to operate the virtual interface (sha0) both in Fast switching and RIP modes at the same time.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m b -i hostc -t hme0,hme1
```

The following shows an example of the setting command used in RIP mode to have each of two virtual interfaces (sha0 and sha1) bundle two of three physical interfaces (hme0, hme1, and hme2) and share one physical interface (hme1) between two virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i hostd -t hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m r -i hoste -t hme1,hme2
```

The following shows an example of the setting command used to define two logical virtual interfaces (sha0:2 and sha0:3) on the virtual interface (sha0).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i hostf -t hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i hostg
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:3 -i hosth
```

The following shows an example of the setting command used to have the virtual interface (sha0) bundle only one physical interface (hme0).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i hosti -t hme0
```

The following shows an example of the setting command used in NIC switching mode to set two physical interfaces (hme0 and hme1) and use the logical IP address takeover function and the standby patrol function (operation mode "p"). Before NIC switching mode can be used, the router/HUB monitoring function must be set.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i hostg -e hosth -t
hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t
sha0
```

The following shows an example of the setting command used in NIC switching mode to set two physical interfaces (hme0 and hme1) and use the physical IP address takeover function and the standby patrol function (operation mode "p"). Before NIC switching mode can be used, the router/HUB monitoring function must be set.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i hosti -t hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t
sha0
```

The following shows an example of the setting command used in GS/SURE linkage mode to have two physical interfaces (hme0 and hme1) bundled. For this purpose, first set the physical interfaces in GS/SURE linkage mode (operation mode "n"), then create virtual interfaces in GS/SURE linkage mode (operation mode "n"), and have the virtual interfaces bundled to set GS/SURE linkage mode (operation mode "c").

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i hostd -t hme0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i hoste -t hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i hostf -t sha1,sha2
```

The following is an example that set two physical interfaces (hme0 and hme1) to use a logical IP address takeover function by an IPv6 address in NIC switching mode. It is necessary to set a router/HUB monitoring function other than this setting.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig inet6 create -n sha0 -m d -i fec0:1::1/64 -t
hme0,hme1
or
# /opt/FJSVhanet/usr/sbin/hanetconfig inet6 create -n sha0 -m d -i hostg/64 -t
hme0,hme1
```

The following is an example of configuring two physical interfaces (hme0 and hme1) and creating a virtual interface (sha0) using IPv6 address.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1
```

The following shows an example of the setting command used in NIC switching mode to set two VLAN interfaces (fjgi1000 and fjgi1001) and use the logical IP address takeover function and the standby patrol function (operation mode "p"). Before NIC switching mode can be used, the router/HUB monitoring function must be set.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i hostg -e hosth -t
fjgi1000,fjgi1001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t
sha0
```

(2) modify command

The following is an example of modifying bundled physical interfaces (hme0 and hme1) in the virtual interface (sha0) to different physical interfaces (hme2 and hme3).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -t hme2,hme3
```

The following is an example of modifying the virtual IP address defined in the virtual interface (sha0).

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

The following is an example of modifying the virtual interface (sha0) to use Fast switching mode and RIP mode concurrently. (This modification is only allowed for Fast switching mode or RIP mode)

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -m b
```

The following is an example of modifying the value of the local MAC address to be allocated in the standby NIC used in NIC switching mode.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha1 -a 02:00:00:00:00:01
```

(3) copy command

The following is an example of sharing the NIC, used in the virtual interface (sha0 for IPv4) for NIC switching mode (operation mode “d”), with another virtual interface (sha2 for IPv4).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha2 -i host4
```

The following is an example of sharing the NIC, used in the virtual interface (sha0 for IPv6) for NIC switching mode (operation mode “d”), with another virtual interface (sha2 for IPv4).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha0 -i host4 –e hostp
```

The following is an example of sharing the NIC, used in the virtual interface (sha0 for IPv6) for NIC switching mode (operation mode “d”), with another virtual interface (sha2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha2 -i host6/64
```

The following is an example of sharing the NIC, used in the virtual interface (sha0) for IPv4) for NIC switching mode (operation mode “d”), with another virtual interface (sha2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i host6/64
```

(4) delete command

The following is an example of deleting the virtual interface (sha2 for IPv4).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n sha2
```

The following is an example of deleting the virtual interface (sha2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete inet6 -n sha2
```

The following is an example of deleting the logical virtual interface (sha0:2).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n sha0:2
```

The following is an example of deleting the logical virtual interface (sha0:2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete inet6 -n sha0:2
```

7.2 strhanet Command

[Name]

strhanet - Activation of virtual interfaces

[Synopsis]

/opt/FJSVhanet/usr/sbin/strhanet [inet | inet6 | dual] [-n devicename1[,devicename2,...]]

[Feature description]

The strhanet command activates virtual interfaces in accordance with the generated configuration information.

[Option]

It is possible to specify the following options:

[inet | inet6 | dual]

Specify an IP address form assigned to a virtual interface to be activated.

Inet	: IPv4 address
inet6	: IPv6 address
dual	: IPv4/IPv6 dual stack configuration

When omitted, virtual interfaces of all forms are to be dealt with. IPv4 and IPv6 addresses are activated at the same time in a virtual interface of dual stack configuration. It is not possible to activate only an IPv4 address or only an IPv6 address respectively. Dual stack configuration in this case does not mean IPv4 and IPv6 addresses are set on each of the stacked physical interfaces, but they are set to one virtual interface defined in a Redundant Line Control function. This option is valid only in Fast switching mode (operation mode is "t") or NIC switching mode (operation mode is "d").

-n devicename1[,devicename2,...]

Specify a virtual interface name to be activated. Multiple virtual interfaces can be specified by delimiting them with a comma (,). Configuration information for virtual interface names specified here must have been generated with the hanetconfig create command. If this option is not specified, all created virtual interfaces are activated.

[Related commands]

hanetconfig
stphanet
dsphanet

[Notes]

- If an additional virtual interface is activated in Fast switching mode, nodes that have been activated in Fast switching mode may be temporarily overloaded.
- This command can activate a virtual interface only if configuration information has already been set by using the hanetconfig command before executing this command. For details, see “Chapter 3 Environment configuration".
- Virtual interfaces used in a cluster system cannot be activated with this command.
- No logical virtual interface can be specified for the -n option. Logical virtual interfaces are automatically activated when corresponding virtual interfaces are activated.
- This command can be specified for virtual interfaces in Fast switching mode (operation mode "t"), RIP mode (operation mode "r"), Fast switching/RIP mode (operation mode "b"), NIC switching mode (operation mode “d” or “e”), and GS/SURE linkage mode (operation mode "c"). This command cannot be specified for virtual interfaces in Standby patrol function (operation mode “p” or “q”), and GS/SURE linkage mode (operation mode "n").
- A standby patrol function ("p" or "q") is automatically activated when activated a virtual interface of the corresponding NIC switching mode ("d" or "e").
- A virtual interface of GS/URE linkage mode ("n") is automatically activated when activated a virtual interface of GS/SURE linkage mode ("c") that bundles this interface.
- To add and activate a virtual interface of the other NIC switching modes ("d" or "e") with

a virtual interface of NIC switching mode ("d" or "e") is already activated, stop temporarily all virtual interfaces of the activated NIC switching mode ("d" or "e") using a stphanet command. Then execute a strhanet command and activate the virtual interfaces.

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

[Examples]

The following is an example in which all virtual interfaces defined in the configuration information for Redundant Line Control function are activated.

```
# /opt/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 possbile 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 opetion 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"), RIP mode ("r"), Fast switching/RIP mode ("b"), NIC switching mode ("d" or "e"), and GS/SURE linkage mode ("c"). It is not possible to specify to a virtual interface of a standby patrol function ("p" or "q") and GS/SURE linkage mode ("n"). A Standby patrol function ("p" or "q") is automatically deactivated when deactivated a virtual interface of the corresponding NIC switching mode ("d" or "e"). A virtual interface of GS/SURE linkage mode ("n") is automatically deactivated when deactivated a virtual interface of GS/SURE linkage mode ("c") that bundles this virtual interface.
- Be sure to use a stphanet command to deactivate a virtual interface. Do not use an ifconfig command to do the operation.
- A virtual interface of standby patrol set after activated NIC switching mode and activated by strptl command is not deactivated. Use stpptl command to deactivate.
- When a virtual interface of NIC switching mode is deactivated and only a virtual interface of standby patrol is activated, use stpptl command to deactivate the virtual interface of standby patrol.

- If the Solaris zone is using the virtual interface, you cannot deactivate it. First, stop the Solaris zone then deactivate the virtual interface by executing the stphanet command.

[Examples]

The following is an example in which all virtual interfaces (excluding virtual interfaces in cluster operation) defined in the configuration information for Redundant Line Control function are inactivated.

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

The following is an example in which only the virtual interface sha2 defined in the configuration information for Redundant Line Control function is inactivated.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha2
```

The following shows an example to inactivate all virtual interfaces of Fast switching mode or NIC switching mode and also in dual stack configuration.

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

7.4 dsphanet Command

[Name]

dsphanet - Displaying the operation status of virtual interfaces

[Synopsis]

/opt/FJSVhanet/usr/sbin/dsphanet [-n devicename1[,devicename2,...] | -o | -c]

[Feature description]

The dsphanet command displays the current operation status of virtual interfaces and logical virtual interfaces.

[Option]

You can specify the following options:

-n devicename1[,devicename2,...]

Specify the name of a virtual interface whose status should be displayed. You can specify more than one virtual interface by listing them delimited with a comma (,). If this option is not specified, this command displays all the virtual interfaces that are properly defined.

-o

Displays all communication parties of virtual interfaces defined in Fast switching mode (operation mode "t"). This option does not display communication parties of virtual interfaces not yet activated using the strhanet command.

-c

Displays the number of assigned connections defined in GS/SURE linkage mode (operation mode "c"). The number of connections is displayed as "-" if the concerned virtual interface is not activated. The number of connections is displayed as "-" also if the communication target monitoring function is not set or no connection is yet established.

[Display format]

The following shows the display formats used when no option is specified and when the -n option is specified.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
 Name       Status   Mode CL   Device
+----------+--------+----+----+----------------------------------------+
 sha0        Active    d   OFF  qfe0(ON),qfe1(OFF)
 sha1        Active    d   OFF  qfe2(OFF),qfe3(ON)
 sha2        Active    t   OFF  hme0(ON),hme1(ON)
 sha3        Active    p   OFF  sha0(ON)
 sha4        Active    q   OFF  sha1(ON)
[IPv6]
 Name       Status   Mode CL  Device
+----------+--------+----+----+----------------------------------------+
 sha0        Active    d   OFF  qfe0(ON),qfe1(OFF)
 sha1        Active    d   OFF  qfe2(OFF),qfe3(ON)
 sha5        Active    t   OFF  hme2(ON),hme3(ON)
```

Item		**Explanation**
[IPv4,Patrol]		Displays virtual interface information of an IPv4 address and standby patrol form.
[IPv6]		Displays virtual interface information of an IPv6 address form.
Name		Outputs a virtual interface name.
Status		Outputs the status of a virtual interface.
Status	Active	Active status
	Inactive	Inactive status
Mode		Outputs the operation mode of a virtual interface.
Mode	t	Fast switching mode
	r	RIP mode
	b	Fast switching/RIP mode
	n	GS/SURE linkage mode (physical interface definition)
	c	GS/SURE linkage mode (virtual interface definition)
	d	NIC switching mode (logical IP address takeover function)
	e	NIC switching mode (physical IP address takeover function)
	p	Standby patrol function (automatic failback if a failure occurs)
	q	Standby patrol function (immediate automatic failback)
CL		Cluster definition status
CL	ON	Cluster resource
	OFF	None cluster resource
Device		Outputs the physical interface names bundled by a virtual interface and, enclosed in parentheses, the statuses of the physical interfaces.
Device	ON	Enabled Displays the status if the interface is enabled and also available. For the standby patrol interface, the status is displayed if the transfer path is valid.
	OFF	Disabled Displays the status if the virtual interface in disabled. For Fast switching and GS/SURE modes, it also displays the status when the failure is detected in the remote systems. In NIC switching mode, it displays the status when the standby patrol function is disabled.
	STOP	Ready for use Displays the status immediately after configuring the environment for NIC switching mode.
	FAIL	Error in one system Displays the status if the failure is detected on standby patrol function.

	CUT	Unused Displays the status if temporally dispatched by hanetnic delete command.
	LOST	System unstable Displays the status when the physical interface is disabled by a third person. NIC switching mode automatically recovers this symptom. However, the other redundant modes require manual recovery.

The following shows the display format used when the -o option is specified.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -o
   NIC    Destination Host Status
+--------+----------------+----------------+
 hme0      hahostA          Active
           hahostB          Active
           hahostC          Inactive
 hme1      hahostA          Active
           hahostB          Active
           hahostC          Inactive
```

Item		**Explanation**
NIC		Outputs a physical interface name.
Destination Host		Outputs the host name of the communication target. (If the target host does not exist, it will display "none".)
Status		Outputs the status of the communication target.
Status	Active	Active status
	Inactive	Inactive status

The following shows the display format used when the -c option is specified.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -c
  Name  IFname Connection
+------+------+----------+
 sha0   sha2        -
        sha1        -
 sha10  sha12       5
        sha11       7
```

Item	**Explanation**
Name	Outputs a virtual interface name in GS/SURE linkage mode (operation mode "c").
IFName	Outputs a virtual interface name in GS/SURE linkage mode (operation mode "n").
Connection	Outputs the number of connections. When a virtual interface is not activated, "-" is displayed. When a function to monitor the other end of communication is not set, or when a connection is not established, "-" is displayed as well.

[Related commands]

strhanet
stphanet

[Notes]

- This command can be specified for any virtual interfaces.
- Only one option can be specified at one time.

[Examples]

The following shows an example of displaying the active or inactive status of all virtual interfaces that are properly defined in the configuration information for Redundant Line Control function.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
```

The following shows an example of displaying all the communication parties of virtual interfaces in Fast switching mode (operation mode "t") properly defined in the configuration information for Redundant Line Control function.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -o
```

The following shows an example of displaying the number of assigned connections of virtual interfaces in GS/SURE linkage mode (operation mode "c") properly defined in the configuration information for Redundant Line Control function.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -c
```

7.5 hanetobserv Command

[Name]

hanetobserv - Setting, modifying, deleting, and displaying the information for the communication target monitoring function

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetobserv command [args]

[Feature description]

The hanetobserv command sets, modifies, deletes, and displays the monitoring destination information required for the operation in GS/SURE linkage mode.

Command	Process outline	Authority
create	Sets a monitoring destination	Super user
print	Displays monitoring destination information	General user
modify	Modifies monitoring destination information	Super user
delete	Deletes monitoring destination information	Super user

(1) create command

The operation in GS/SURE linkage mode requires the monitoring of the communication target. This enables the system to continue communication using other communication paths when a failure occurs. Use the create command to generate a communication target. The following is the command format for generating a monitoring destination:

GS communication (If adding ipaddress):
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddress -t nicaddress1[,nicaddress2,...] -m {on | off} [-r {on | off}]

GS communication (If adding more nicaddress to an already defined ipaddress):
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddress -t nicaddress3[,nicaddress4,...]

SURE communication (using SURE communication function):
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddress -t nicaddress1:pm-id[,nicaddress2:pm-id,...] -m {on | off} [-r {on | off}]

SURE communication (using TCP relay function):
/opt/FJSVhanet/usr/sbin/hanetobserv create -i ipaddress -c clientaddress1[:subnetmask][,clientaddress2[:subnetmask],...]

-n node:

Specify a name by which to identify the node of a communication target, using up to 16 one-byte characters.

-i ipaddress:

Specify a host name or IP address of a virtual interface held by the communication target. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts and /etc/inet/ipnodes files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation.

-t nicaddress1[:pm-id][,nicaddress2[:pm-id],...]:

Specify the host names or IP addresses of physical interfaces bundled by a virtual interface, by listing them delimited with a comma (,).

nicaddressX:

Specify the host name or IP address of a physical interface bundled by a virtual interface.

pm-id:

Specify the identifier of the PM (processor module) group to which the physical interface of the communication target belongs when it is the SURE system. Specify a number from 1 to 8. This option is not required if the communication target is GS.

-m on | off:

Set whether or not to monitor the virtual interface of the monitoring destination that has been set.

Since the local host need not monitor the communication target if the remote host monitors it, specify a mode depending on the setting of the remote host.

In hot standby configuration (GS), specify this parameter only on one of the active and standby nodes when their monitoring destination information is defined.

on:

The local host monitors the communication target.

off:

The local host does not monitor the communication target.

-r on | off:

Sets if or not a RIP packet is sent from the other device. It is possible to omit this option. When omitted, RIP sending on (ON) is set. When GS has a hot standby configuration, define this parameter only in one node at setting the monitor-to information of an operation node or a standby node.
Notes)
Be sure to set RIP to "on" in order to decide which of an operation node or a standby node is working by RIP when the other system has a hot standby configuration.

on:

When sending a notification of node switching to the other system, it sends a notification of node switching waiting for receiving RIP from the other system.

off:

When sending a notification of node switching to the other system, it sends a notification of node switching to all routes without waiting for receiving RIP from the other system.

-c clientaddress1[:subnetmask][,clientaddress2[:subnetmask],...]:

Specify the communication parties and destination networks with which communication should be performed using the virtual interface of the relay destination, by listing them delimited with a comma (,).

clientaddressX:

Specify the host name or IP address of a remote host or network with which communication should be actually performed. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts and /etc/inet/ipnodes files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation. If a remote network is specified, a "subnetmask" must be specified.

subnetmask:

This option must be specified when a remote network is specified in "clientaddressX". Specify the subnet mask value of the network in dotted decimal notation.

(2) print command

Use the print command to display the current monitoring destination information. The following is the format of the print command. If no option is specified, information on both the monitoring destination and the relay destination is output.

```
/opt/FJSVhanet/usr/sbin/hanetobserv print [-o] [-c]
```

-o:

Specify this option to output information on only the monitoring destination.

-c:

Specify this option to output information on only the relay destination.

The following shows an example of displaying monitoring destination information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
 Destination Host Virtual Address  POLL RIP  NIC Address(:PMgroupID)
+----------------+----------------+----+----+--------------------------------+
 hahostA          ipaddressB       ON   OFF  ipaddressC,ipaddressD
                                             ipaddressE,ipaddressF
 hostB            ipaddressG       ON   ON   ipaddressH:1,ipaddressJ:1

 Virtual Address  Client Address
+----------------+------+-------------------------------------------------+
 ipaddressG       host   ipaddressK
                  net    10.0.0.0:255.0.0.0
```

Item		**Explanation**
Destination Host		Outputs the host name of the communication target.
Virtual Address		Outputs the virtual interface name.
POLL		Outputs the monitoring mode.
RIP		With or without an RIP packet sent from the other end device.
POLL	ON	The local host monitors the communication target.
	OFF	The local host does not monitor the communication target.
RIP	ON	With an RIP packet sent from the other host.
	OFF	Without an RIP packet sent from the other host.
NIC Address(:PMgroupID)		Outputs the IP address or host name of a physical interface bundled by a virtual interface. An ID value is shown in parentheses.

Item		**Explanation**
Virtual Address		Outputs the virtual interface name.
Client		Outputs the network type of the communication destination.
Client	host	Indicates that the host address of the communication destination is output in "Address".

	net	Indicates that the network address of the communication destination is output in "Address".
Address		Outputs address information of the communication destination.

(3) modify command

Use the modify command to modify the monitoring destination information generated using the create command. The following is the format of the modify command:

```
/opt/FJSVhanet/usr/sbin/hanetobserv modify -n node,new-node |
    -n node -i ipaddress,new-ipaddress |
    -n node -i ipaddress -t nicaddress,new-nicaddress1[:pm-id][,new-nicaddress2[:pm-id],...] |
    -n node -i ipaddress {-m {on | off} | -r {on | off}} |
    -i ipaddress -c clientaddress[:subnetmask],new-clientaddress[:subnetmask]
```

-n node,new-node:

Specify the node name of the monitoring destination information to be modified.

node:

Specify a node name that is set in the monitoring destination information (to be modified).

new-node:

Specify a node name to be used after modification.

If this parameter is specified, none of parameters "-i", "-t", and "-m" needs to be specified.

-i ipaddress,new-ipaddress:

Specify a host name or IP address of a virtual interface of the monitoring destination information to be modified. This parameter cannot be specified at the same time as when the node name or operation mode is modified.

ipaddress:

Specify a host name or IP address that is set in the monitoring destination information (to be modified).

new-ipaddress:

Specify a host name or IP address to be used after modification.

If this parameter is specified, none of new-node in parameter "-n" and parameters "-t" and "-m" needs to be specified.

-t nicaddress,new-nicaddress1[:pm-id][,new-nicaddress2[:pm-id],...]:

Specify the IP address or host name of physical interfaces bundled by a virtual interface of the monitoring information to be modified. This parameter cannot be specified at the same time as when the node name, host name or IP address of the virtual interface, or operation mode is modified.

nicaddress:

Specify the first IP addresses or host names in the IP address or host name list that bundles physical interface that are set in the monitoring destination information (to be modified). Check the first real interface names using the print command of hanetobserv.

If the monitoring target data displayed from executing "hanetobserv print" command contains "ipaddressC,ipaddressD" under "NIC Address(:PMgroupID)" section, in such a case, use the headmost entry or "ipaddressC".

new-nicaddress1[:pm-id][,new-nicaddress2[:pm-id],...]:

Specify all the IP address or host name of a physical interface to be bundled after modification, by listing them delimited with a comma (,).

If this parameter is specified, none of new-node in parameter "-n", new-ipaddress in parameter "-i", and parameter "-m" needs to be specified.

new-nicaddressX:

Specify the host name or IP address of interfaces to be bundled by a virtual interface.

pm-id:

Specify the identifier of the PM (processor module) group to which the physical interface of the communication target belongs when it is the SURE system. Specify a number from 1 to 8. This option is not required if the communication target is GS.

-m on | off:

Specify the operation mode of the monitoring destination information to be modified.
This parameter cannot be simultaneously specified, when changing other parameters.

-r on | off:

Specify the existence of the RIP transmission from a remote system.
This parameter cannot be simultaneously specified, when changing other parameters.

-c clientaddress[:subnetmask],new-clientaddress[:subnetmask]:

Modify the host name or IP address of the party with which communication should be actually performed. If a subnet mask value is specified in the information to be modified, the subnet mask value must be specified for modification.

clientaddress[:subnetmask]:

Specify the client information to be modified. If a subnet mask value is specified in the information that has been defined, the subnet mask value must be specified.

new-clientaddress[:subnetmask]:

Specify the client information to be used after modification. To specify a network, the subnet mask value must be specified.

(4) delete command

The following is the format of the delete command used to delete the monitoring destination information created using the create command:

```
/opt/FJSVhanet/usr/sbin/hanetobserv delete -n all |
        -n node1[,node2,...] |
        -n node -i ipaddress1[,ipaddress2,...] |
        -n node -i ipaddress -t nicaddress1[:pm-id][,nicaddress2[:pm-id],...] |
        -c all |
        -i ipaddress -c all |
        [-i ipaddress] -c clientaddress1[:subnetmask][,clientaddress2[:subnetmask],...]
```

-n all:

If all is specified, all monitoring destination information is deleted.

-n node1[, node2, ...]:

Specify a remote node name or IP address that is set in the monitoring destination information and should be deleted. You can specify more than one remote node name or IP address by listing them delimited with a comma.

-n node -i ipaddress1[,ipaddress2,...]:

Delete the virtual interface information under the node information that is set in the monitoring destination information. Specify a node name or virtual IP address attached to the virtual

interface under the remote node name to be deleted. You can specify more than one node name or IP address by listing them delimited with a comma. If only one virtual interface is defined under node, the node definition information is also deleted.

-n node -i ipaddress -t nicaddress1[:pm-id][,nicaddress2[:pm-id],...]:

This command deletes the list of IP addresses or host names of physical interface assigned under virtual interface. Specify the host name or IP address of the physical interface you wish to delete. It is possible to specify more than one name or IP addresses by separating them with comma.
In the case where a single list of hostname or IP address of the physical interface is defined, the virtual interface will be deleted as well. Furthermore, if only one virtual interface is defined under the node, the configuration data including the mutual interface will be deleted as well. The host name or IP address or the physical interface can be verified using hanetobserv print command.

-c all

Delete the definition that is set to use the TCP relay function.

-i ipaddress -c all

Delete all the information under the virtual interface information specified in the "-i" option.

[-i ipaddress] -c clientaddress1[:subnetmask][,clientaddress2[:subnetmask],...]

Delete all the real NIC information to be relayed. Specify the "-i" option to delete only the real NIC information under a specific virtual interface. You can specify more than one NIC by listing them delimited with a comma.

[Notes]

- Configuration information must be defined before a monitoring destination is created.
- This command can be set if a virtual interface in GS/SURE linkage mode (operation mode "c") is defined.
- To add, delete, or change a monitoring destination, the virtual interface in GS/SURE linkage mode (operation mode "c") must be inactivated.
- No monitoring destination registered in a cluster can be deleted or changed. First release the cluster definition and then delete or change the monitoring destination.
- An IP address or host name to be specified when the communication target monitoring function is set or changed must be defined in /etc/inet/hosts and /etc/inet/ipnodes.
- The node name information must not be specified as "all".
- Up to 32 physical interfaces can be specified to be bundled by the virtual interface of the communication target to be specified in the monitoring destination information.
- When specified a numeric string for a host name, it is dealt with as decimal and converted into an IP address corresponding to its value to work. (For instance, when specified "123456", it is regarded an IP address "0.1.226.64" is specified.)
- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change the corresponding host name on the host database of such as /etc/inet/hosts and /etc/inet/ipnodes files. To change the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.
- Do not use characters other than alphanumeric characters, period, and hyphen for the host name. If characters other than the above are used, re-write the host names in /etc/inet/hosts and /etc/inet/ipnodes so that it does not contain any other characters. Also, the first and last character for the host name must be alphanumeric character.

[Examples]

(1) create command

The following shows a setting example in which monitoring is performed while the communication target's node hahostA has virtual IP address “vip1”, which bundles two physical IP address ipaddressC and ipaddressD. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip1 -t
ipaddressC,ipaddressD -m on
```

The following shows a setting example in which monitoring is not required because the already defined communication target hahostA has virtual IP address “vip2”, which bundles physical IP address ipaddressF and ipaddressG. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip2 -t
ipaddressF,ipaddressG -m off
```

The already defined communication target hahostA has virtual IP address “vip2”, which bundles two physical IP addresses ipaddressF and ipaddressG. The following shows a setting example in which new physical IP addresses ipaddressH and ipaddressJ are bundled and added to virtual IP address “vip2”. The system takes over the monitoring mode used when physical IP addresses ipaddressF and ipaddressG are set. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip2 -t
ipaddressH,ipaddressJ
```

Define the SURE interface to be used to communicate with the node of the communication target when the TCP relay function in GS/SURE linkage mode is used. The SURE virtual IP address “vip2” to be used is assumed to be already defined. The following shows a setting example in which a network (10.0.0.0) is added to the communication target. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -i vip2 -c 10.0.0.0:255.0.0.0
```

(2) print command

The following shows an example of displaying the configuration information list of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
```

(3) modify command

The following shows an example of changing the node name (hahostB) in the communication target monitoring destination information to hahostH.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB,hahostH
```

The following shows an example of changing the virtual IP address “vip1” of the node (hahostB) in the communication target monitoring destination information to “vip2”.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip1,vip2
```

The following shows an example of changing the physical IP addresses (ipaddress1 and ipaddress2) bundled by virtual IP address “vip1” of the node (hahostB) in the communication target monitoring destination information to ipaddress3, ipaddress4, and ipaddress5.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip1 -t
ipaddress1,ipaddress3,ipaddress4,ipaddress5
```

The following shows an example of changing the physical IP addresses (ipaddress6 and ipaddress7) bundled by virtual IP address “vip2” of the node (hahostB) in the communication target monitoring destination information to ipaddress7 and ipaddress8.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip2 -t
ipaddress6,ipaddress7,ipaddress8
```

The following shows an example of changing the "on" setting of the monitoring mode of the node (hahostB) in the communication target monitoring destination information to "off".

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -m off
```

The following shows an example of changing the communication target (ipaddress6) in the relay destination information (ipaddress6 and ipaddress7) of the virtual IP address “vip2” in the communication target monitoring destination information to a network specification (10.0.0.0, 255.0.0.0).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -i vip2 -c
10.0.0.0:255.0.0.0,ipaddress7
```

(4) delete command

The following shows an example of deleting all the monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n all
```

The following shows an example of deleting all the information held by the monitored host (hahostA).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n hahostA
```

The following shows an example of deleting the information under the virtual IP address “vip1” held by the monitored host (hahostA).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n hahostA -i vip1
```

The following shows an example of deleting the information under the virtual IP address “vip1” held by the monitored host (hahostA).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n hahostA -i vip1
```

The following shows an example of deleting the physical IP addresses (ipaddressC, ipaddressD) under the virtual IP address “vip1” in the TCP relay information.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -i vip1 -c ipaddressC,ipaddressD
```

7.6 hanetparam Command

[Name]

hanetparam - The setting value of various functions is changed or displayed

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetparam {-w sec | -m times | -l times | -p sec | -o times | -d {plumb | unplumb} | -c {on | off} | -s {on | off}}
/opt/FJSVhanet/usr/sbin/hanetparam print

[Feature description]

The hanetparam command sets up the monitoring function when the Fast switching operation or the standby patrol function is used. This command also changes the method of activating and inactivating Fast switching mode and NIC switching mode.

[Option]

You can specify the following options:

< Valid options in fast switching mode >

-w value

Specify the interval (value) for monitoring the communication target in Fast switching mode. A value from 0 to 300 can be specified. No monitoring is performed if 0 is specified in value. By default, 5 is specified. This parameter is enabled only for Fast switching mode.

-m value

Specify the monitoring retry count (value) before message output when the message output function for a line failure is enabled.

Specify the monitoring retry count (value) before message output. A value from 0 to 100 can be specified. No message is output if 0 is specified in value. By default, no message is output. This parameter is enabled only for Fast switching mode.

-l value

Specify the cluster failover function.

Specify how many times (count) communication with the communication target can fail consecutively before cluster failover is performed. A value from 0 to 100 can be specified. No cluster failover is performed if 0 is specified in value. When performing cluster failover, the number of times for repeating surveillance is specified in the range from 1 time to 100 times until it cluster failover. By default, cluster failover is specified to be performed if communication fails five consecutive times. This parameter is enabled only for Fast switching mode on a cluster system.

-c value

When operating Fast switching mode on a cluster system and when an error occurred in all transfer routes at the activation of a userApplication, sets if or not to execute failover between clusters (job switching between nodes).
Specify "on" to value for executing failover between clusters (job switching between nodes) when an error occurred in all transfer routes at activation of a userApplication.
Specify "off" to value for not executing failover between clusters when an error occurred in all transfer routes at activation of a userApplication.
"off" is set to value as an initial setting value.

-s value

Specify if or not to output a message when a physical interface, which a virtual interface uses, changed the status (detected an error in a transfer route or recovery). A value possible to specify is "on" or "off". When specified "on", a message is output (message number: 990, 991, and 992). When specified "off", a message is not output. The initial value is "off". This parameter is valid only in fast switching mode.

< Valid options in NIC switching mode >

-p value

Specify the interval (value) for monitoring the communication target when the standby patrol function is enabled. A value from 0 to 100 can be specified. No monitoring is performed if 0 is specified in value.
Do not specify 0 to this parameter when set a user command execution function (executing a user command when standby patrol detected an error or recovery). User command execution does not function if specified 0.
By default, 15 is specified. This parameter is enabled only for NIC switching mode.

-o value

Specify the monitoring retry count (value) before message output when the message output function for a standby patrol failure is enabled.
Specify the monitoring retry count (value) before message output. A value from 0 to 100 can be specified.
When specified 0, stop outputting messages and make monitoring by a standby patrol function invalid. Do not specify 0 to this parameter when set a user command execution function (executing a user command when standby patrol detected an error or recovery). User command execution does not function, if specified 0.
By default, 3 is specified. This parameter is enabled only for NIC switching mode. The number of the times of continuous monitoring is "a set value of this option x 2" immediately after started standby patrol.

-d value

Use this parameter to change the method of inactivating the standby interface in NIC switching mode. Specify "plumb" in value to inactivate the standby interface and set "0.0.0.0" as the IP address. This procedure allows "INTERSTAGE Traffic Director", etc. to be used as the host application. Alternatively, specify "unplumb" in value to inactivate and delete the standby interface. Initially, "unplumb" is specified in value. If you specify a physical interface of NIC switching for the network setting of the Solaris container (zone), be sure to specify "plumb" for the parameter. If the Solaris zone is started without the "plumb" setting, Solaris zone startup will fail because the physical interface (standby interface) has not been used. Specifying "plumb" will deactivate the standby interface after NIC switching so that zone startup will properly be performed.

Setting	**Interface**					
	Operating			**Standby**		
	Status	**IP address**	**Allocation of logical I/F**	**Status**	**IP address**	**Allocation of logical I/F**
unplumb	Active	Yes	Possible	Unused	-	Impossible
plumb	Active	Yes	Possible	Inactive	None (0.0.0.0)	Possible

< Valid options in all modes >

print:

Outputs a list of settings.

The following shows the output format:

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
   Line monitor interval(w)           :5
   Line monitor message output (m)    :0
   Cluster failover (l)               :5
   Standby patrol interval(p)         :15
   Standby patrol message output(o)   :3
   NIC switching mode(d)              :Unplumb
   Cluster failover in unnormality (c):OFF
   Line status message output (s)     :OFF
```

Item		**Explanation**
Line monitor interval (w)		Outputs the setting for the transmission line monitoring interval.
Line monitor message output (m)		Outputs the monitoring retry count before message output when a line failure occurs.
Cluster failover (l)		Outputs the consecutive monitoring failure count before execution of cluster failover.
Standby patrol interval (p)		Outputs the monitoring interval of the standby patrol.
Standby patrol message output (o)		Outputs the consecutive monitoring failure count before output of a message when a standby patrol failure occurs.
NIC switching mode (d)		Outputs the method of inactivating the standby interface in NIC switching mode.
NIC switching mode (d)	Unplumb	Inactivates the standby interface and deletes.
	Plumb	Inactivates the standby interface and sets the IP address as "0.0.0.0".
Cluster failover in unnormality(c)		Workings when an error occurred in all transfer routes at activating a userApplication.
Cluster failover in unnormality(c)	ON	Cluster switching immediately occurs.
	OFF	Cluster switching does not occur at activating a userApplication.
Line status message output (s)		With or without a message output when a physical interface changed the status.
Line status message output (s)	ON	A message is output.
	OFF	A message is not output.

[Related command]

hanetpoll

[Notes]

- This command can be specified for a virtual interface in Fast switching mode (operation mode "t"), NIC switching mode (operation mode "d" or "e"), and standby patrol function (operation mode "p" or "q").
- The setting by this command is valid in the whole system. It is not possible to change in a unit of virtual interface.
- After executing this command, reboot the system immediately. The applied value will not be effective until the system restarts.

[Examples]

< Example of Fast switching mode >

(1) Example of setting 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
```

(3) Example of changing the method of inactivating the standby interface

The following shows an example of using this command to inactivate the standby interface and set "0.0.0.0" as the IP address (using "INTERSTAGE Traffic Director", Solaris Containers, etc. as the host application).

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d plumb
```

< Example common to all modes >

(1) Example of executing the status display command

The following shows an example of displaying the settings made using the hanetparam command.

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
```

7.7 hanetpoll Command

[Name]

hanetpoll - Setting, modifying, deleting, and displaying the monitoring destination information for the Router/HUB monitoring function

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetpoll command [args]

[Feature description]

The hanetpoll command sets the monitoring destination information required for the Router/HUB monitoring function. This command also modifies, deletes, displays, enables, or disables the settings.

command	Process outline	Authority
create	Creates monitoring destination information	Super user
copy	Copies monitoring destination information (synchronous switch)	Super user
print	Displays monitoring destination information	General user
modify	Modifies monitoring destination information	Super user
delete	Deletes monitoring destination information	Super user
on	Enabling the Router/HUB monitoring function	Super user
off	Disabling the Router/HUB monitoring function	Super user

(1) create command

The operation of the router/HUB monitoring function requires the definition of monitoring destination information. Use the create command to define monitoring destination information.

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n devicename -p
polladdress1[,polladdress2] [-b {on | off}]
```

-n devicename:

Specify the name of a virtual interface to be monitored. Specify a virtual interface created using the hanetconfig create command or the hanetconfig copy command. No logical virtual interface name can be specified.

-p polladdress1[,polladdress2]:

Specify a monitor-to host name or IP address. Specify a monitor-to host name or IP address to "polladdress1" when activating a Primary interface. Specify a monitor-to host name or IP address to "polladdress2" when activating a Secondary interface. When Primary and Secondary interfaces monitor the same thing, or when a Secondary interface is not defined (a single case), omit "polladdress2". In RIP mode, specify a host name or an IP address of an adjacent router. In NIC switching mode, specify a host name or an IP address of the connected HUB. It is also possible to set IPv4 or IPv6 addresses as an address form. When setting an IPv6 address, do not specify a prefix value. When specifying a host name, do not use the same name that exists in IPv4 and IPv6. If the same name exists, it is dealt with as an IPv6 host.

-b on | off:

If two HUBs are specified as monitoring destinations in NIC switching mode, communication between the primary and secondary HUBs can be monitored.

on: Monitors communication between two HUBs.
off: Does not monitor communication between two HUBs.

(2) copy command

Use this command when copying monitoring target's information to a virtual interface on NIC Switching mode or when synchronizing the switching operation of virtual interface.
This command thus allows monitoring destination information to be automatically created by using the copy source information and without requiring you to specify monitoring destination information and HUB-to-HUB monitoring mode. This command realizes simpler operation than directly executing the hanetpoll create command. The following is the command format for the copy command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n devicename1,devicename2
```

If you have used tagged VLAN interface on NIC Switching mode and created more than one virtual interface, which have disparate network address, you must keep in account that multiple IP address cannot be configured as monitoring target on Switch/HUB running VLAN. In such a case, it is possible to implement synchronous switching in between virtual interfaces using the same physical interface. This allows a virtual interface, which does not have the IP address for monitoring target to perform fail back operation by synchronizing with a virtual interface, which already has the existing monitoring target. In order to synchronize the switching operation of virtual interface, use the "copy" command (it is possible to specify disparate network addresses).

-n devicename1,devicename2:

Specify the names of virtual interfaces from and to which monitoring destination information should be copied.

devicename1:

Specify the name of a virtual interface that is set in monitoring information in the copy source.

devicename2:

Specify the name of a new virtual interface to be monitored. Specify a virtual interface created using the hanetconfig create command or the hanetconfig copy command. No logical virtual interface name can be specified.

(3) print command

Use the print command to display the current monitoring destination information. Use this command to view the current monitoring destination information. The following is the format of the print command.

```
/opt/FJSVhanet/usr/sbin/hanetpoll print [-n devicename1[,devicename2,...]]
```

-n devicename1[,devicename2,...]:

Specify the names of virtual interfaces whose monitoring destination information should be displayed. If this option is not specified, the print command displays all the monitoring destination information currently specified.

The following shows an example of displaying information without any option specified.

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

[ Polling Parameter of each interface ]
 Name    Hostname/Polling Parameter
+-------+-------------------------------------------------------------+
 sha0    swhub1,swhub2
        hub-hub poll       =    OFF
        interval(idle)     =      5( 60) sec
        times              =      5 times
        max_retry          =      5 retry
        repair_time        =      5 sec
        failover mode      =    YES

 Name    Hostname/Polling Parameter
+-------+-------------------------------------------------------------+
 sha1    swhub3,swhub4
        hub-hub poll       =    OFF
        interval(idle)     =      5( 60) sec
        times              =      5 times
        max_retry          =      5 retry
        repair_time        =      5 sec
        failover mode      =    YES
```

Item		**Explanation**
Standard Polling Parameter		Common monitoring information
Polling Parameter of each interface		Each monitoring information
Name		Displays the name of a virtual interface to be monitored.
Hostname		Displays the host name or IP address to be monitored, in the order of the primary and secondary monitoring destinations.
hub-hub poll		Displays the inter-HUB monitoring status.
hub-hub poll	ON	The monitoring function is enabled.
	OFF	The monitoring function is disabled.
	---	The monitoring function is not used.
interval(idle)	interval	Displays the monitoring interval in the stationary status.
	idle	Displays in seconds the wait time that elapses after monitoring starts and before the HUB links up.
times		Displays the monitoring count.
max_retry		Displays the consecutive failure occurrence

		count before failure notification.
repair_time		Displays the recovery monitoring interval in seconds.
failover mode		With or without cluster switching when an error occurred in all transfer routes.
failover mode	YES	Node switching is performed when the virtual interface is registered in the cluster resource.
	NO	No node switching is performed.

(4) modify command

Use the modify command to modify the monitoring destination information.

```
/opt/FJSVhanet/usr/sbin/hanetpoll modify -n devicename {[-p polladdress1[,polladdress2]] [-b {on | off}]}
```

-n devicename:

Specify the name of a virtual interface whose monitoring destination information should be modified. Specify a virtual interface whose monitoring destination information is currently defined.

-p polladdress1[,polladdress2]:

Specify the host names or IP addresses of the monitoring destinations to be modified. In RIP mode, specify the host names or IP addresses of neighboring routers as the monitoring destinations. In NIC switching mode, specify the host names or IP addresses of the primary and secondary HUBs.

-b on | off:

If two HUBs are specified as monitoring destinations in NIC switching mode, communication between the primary and secondary HUBs can be monitored. This parameter cannot be specified for the monitoring destination information in RIP mode.

on: Monitors communication between two HUBs.
off: Does not monitor communication between two HUBs.

Changing the number of monitoring target from two targets to one target, verify that HUB-to-HUB monitoring exists, and if the value is set "on", then change it back to "off".

(5) delete command

Use the delete command to delete the monitoring destination information. The following is the format of the delete command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll delete -n {devicename1[,devicename2,...] | all}
```

-n devicename1[,devicename2,...]:

Specify the names of virtual interfaces (such as sha0 and sha1) whose monitoring destination information should be deleted.

all:

Specify this parameter to delete all the defined monitoring destination information.

(6) on command

To make the created Router/HUB monitoring function valid, and to change an interval to monitor a Router/HUB monitoring function, and a monitoring function of the other end of communication in GS/SURE linkage mode, use the on command:

RIP mode, Fast switching/RIP mode, NIC switching mode or GS/SURE linkage mode:
/opt/FJSVhanet/usr/sbin/hanetpoll on [-s sec] [-c times] [-r retry] [-b sec] [-f {yes | no}] [-p sec]

NIC switching mode (When a specific virtual interface is specified):
/opt/FJSVhanet/usr/sbin/hanetpoll on -n devicename [-d] | [[-s sec] [-c times] [-b sec] [-f {yes | no}] [-p sec]]

-n devicename:

Specify the virtual interface name (such as sha0, sha1) used in NIC switching mode for enabling HUB monitoring feature. If this option is not specified, the entire virtual interfaces, which have the monitoring target configured, will be selected. In addition, the virtual interface which is sharing NIC synchronizes and enables a HUB monitoring function.

-d:

Changes the value of individually modified monitoring information such as monitoring period and monitoring frequency, into the configuration values that are defined in the common monitoring information. However, this option is only available when '-n' option was individually specified for the virtual interface on NIC Switching mode. (For details on common monitoring information, see the display format of (3) print command)

-s sec:

Specify the monitoring time in seconds. A value from 1 to 300 can be specified (note that the product of sec and times must be 300 or less). If this option is not specified, the previous setting is enabled. Initially, 5 (seconds) is specified.

-c times:

Specify the monitoring count. A value from 1 to 300 can be specified (note that the product of sec and times must be 300 or less). If this option is not specified, the previous setting is enabled. Initially, 5 (times) is specified.

-r retry:

Specify the retry count at which the router monitoring should be stopped when a failure is detected. A value from 0 to 99999 can be specified. If this option is not specified, the previous setting is enabled. Initially, 5 (times) is specified. Specify 0 if the router monitoring should not be stopped.

Only in the case of RIP mode or Fast switching/RIP mode, this option is effective. In the case of other modes, it is ignored.

-b sec:

When detected an error in HUB-to-HUB monitoring of NIC switching mode, and in monitoring the other end of communication in GS/SURE linkage mode, specify an interval to monitor recovery. The range possible to set is zero to 300. If not specified this option, the values set the last time become valid. 5 (seconds) is set as the initial set value.

-f yes | no:

Specify the operation used when node switching occurs due to a line failure during cluster operation. If this option is not specified, the previous setting is enabled. Initially, "yes" is specified. (This parameter is enabled only during cluster operation.)

yes: Node switching is performed if a line monitoring failure occurs.
no: No node switching is performed if a line monitoring failure occurs.

-p sec:

Specify in seconds the wait time that should elapse after monitoring starts and before the HUB links up in RIP mode, NIC switching mode, and GS/SURE linkage mode. A value from 1 to 300 can be specified. If this option is not specified, the previous setting is enabled. Initially, 60 (seconds) is specified. If the specified value is less than 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.

(7) off command

Use the off command to disable the router/HUB monitoring function. The following is the format of the off command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll off [-n devicename]
```

-n devicename:

Specify the virtual interface name (such as sha0, sha1) used in NIC switching mode for disabling HUB monitoring feature. If this option is not specified, the entire virtual interfaces, which have the monitoring target configured, will be chosen. In addition, the virtual interface which is sharing NIC synchronizes and disables a HUB monitoring function.

[Notes]

- Be sure to specify address information for neighboring routers (routers in the subnet to which physical interfaces bundled by the specified virtual interface belong) as the router monitoring destination. If any other address information is specified, the router monitoring function (RIP mode) 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 RIP mode (operation mode "r"), Fast switching/RIP mode (operation mode "b"), and NIC switching mode (operation mode "d" or "e"). (In GS/SURE linkage mode, only the functions of enabling and disabling the monitoring function are available.)
- When modifying the monitoring target data on RIP mode, you must first disable the Router Monitoring feature (hanetpoll off), and then enable the Router Monitoring feature using "hanetpoll on" command.
- A virtual interface to be used in the cluster system is monitored only while a userApplication to which the virtual interface belongs is in operation.
- The monitoring of a Routers/HUBs is not performed when a Router/HUB monitoring function is specified to virtual interface in Fast switching mode. In this case, an error message is output to indicate this fact and the Routers/HUBs is not monitored.
- The monitoring time and count to be specified using the hanetpoll on command must be specified so that their product does not exceed 300.
- The retry count to be specified using the hanetpoll on command can be set to 0 from 99999. Monitoring continues indefinitely if 0 is specified.
- Use the hanetpoll print command to display the latest user-defined information (result of create, delete, modify, on, and off) but not to display the current status of router monitoring.
- If any valid monitoring destination information exists, monitoring automatically starts when the system is started up.
- Be sure to define in the /etc/inet/hosts file IP addresses and host names to be specified when the monitoring destination information is set or modified.
- When specified a numeric string for a host name, it is dealt with as decimal and converted into an IP address corresponding to its value to work. (For instance, when specified "123456", it is regarded an IP address "0.1.226.64" is specified.)
- When setting the same monitor-to device for the monitor-to information of more than one virtual interface, use a copy command, for setting the second and after.
- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts and /etc/inet/ipnodes files. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.

- When specified a host name with this command to where a host name or an IP address should be set, it is not possble to change a corresponding host name on the database such as /etc/inet/hosts and /etc/inet/ipnodes files. To change host name information, it is necessary to delete the definition of a Redundant Line Control function that uses a corresponding host name, and to reset.
- Do not use characters other than alphanumeric characters, period, and hyphen for the host name. If characters other than the above are used, re-write the host names in /etc/inet/hosts and /etc/inet/ipnodes so that it does not contain any other characters. Also, the first and last character for the host name must be alphanumeric character.

[Examples]

(1) create command

The following shows an example of creating configuration information for monitoring two routers routerA and routerB on virtual interface sha2. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha2 -p routerA,routerB
```

(2) copy command

The following is an example of copying monitoring target data defined in virtual interface sha0 for NIC Switching mode into sha1. (By copying the configuration data of sha0 onto sha1, when sha0 performs failover operation, sha1 also fails back along with sha0).

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

(3) print command

The following shows an example of displaying the configuration information list of a virtual interface.

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

(4) modify command

The following shows an example of changing configuration information for monitoring two routers routerA and routerB to routerA and routerC on virtual interface sha2. The host name is assumed to be associated with the virtual IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha2 -p routerA,routerC
```

(5) delete command

The following shows an example of deleting the monitoring destination information on virtual interface sha2 from the definition.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll delete -n sha2
```

(6) on command

The following shows an example of starting the router/HUB monitoring function.

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

The following is an example of starting HUB monitoring function specifying the virtual interface sha0 for NIC Switching mode.

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

(7) off command

The following shows an example of stopping the router/HUB monitoring function.

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

The following is an example of stopping HUB monitoring function specifying the virtual interface sha0 for NIC Switching mode.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off -n sha0
```

7.8 dsppoll Command

[Name]

dsppoll - Displaying the monitoring status

[Synopsis]

/opt/FJSVhanet/usr/sbin/dsppoll [-n devicename | -c]

[Feature description]

The dsppoll command displays the current monitoring status of monitoring information created using the hanetpoll or hanetobserv command.

[Option]

You can specify the following options:

-n devicename:

Specify virtual interface name for RIP, Fast Switching/RIP, or NIC Switching modes. If this option is not specified, the entire interface, which has monitoring target configured will be chosen.

-c:

When this option is specified, displays monitoring information in GS/SURE linkage mode (operation mode "c").

[Display format]

The following is a display format example of when specifying or not specifying virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
+------+-------------------------------------------------------------------------+
 sha0   Polling Status    =     ON
        Primary Target(status)   = swhub1(ON)
        Secondary Target(status) = swhub2(WAIT)
        HUB-HUB status    =    OFF
        interval(idle)    =      5( 60)   times             =      5
        repair_time       =      5        retry             =      5
        FAILOVER Status   =    YES
+------+-------------------------------------------------------------------------+
 sha1   Polling Status    =     ON
        Primary Target(status)   = swhub3(ON)
        Secondary Target(status) = swhub4(WAIT)
        HUB-HUB status    =    OFF
        interval(idle)    =      5( 60)   times             =      5
        repair_time       =      5        retry             =      5
        FAILOVER Status   =    YES
+------+-------------------------------------------------------------------------+

# /opt/FJSVhanet/usr/sbin/dsppoll -n sha0

 Polling Status    =  ON
 interval          =   5
 idle              =  60
 times             =   5
 retry             =   5
 repair_time       =   5
 failover mode     = YES
 Status  Name  Mode Primary Target/Secondary Target             HUB-HUB
+------+------+----+-----------------------------------------+-------+
   ON   sha0    d   swhub1(ON)/swhub2(WAIT)                     OFF
```

Item		**Explanation**
Polling Status		Displays the current status of the monitoring function.
Polling Status	ON	The monitoring function is enabled.
	OFF	The monitoring function is disabled.
interval		Displays in seconds the monitoring interval in the stationary status.
idle		Displays in seconds the wait time that elapses after monitoring starts and before the HUB links up.
times		Displays the monitoring count.
retry		Displays the retry count at which router monitoring should be stopped if a failure is detected. This parameter is meaningless for a virtual interface in NIC switching mode (operation mode "d" or "e") because "1" is set for it.

repair_time		Displays the recovery monitoring interval in seconds.	
FAILOVER Status or failover mode		With or without cluster switching when an error occurred in all transfer routes.	
FAILOVER Status or failover mode	YES	Node switching is performed when the virtual interface is registered in the cluster resource.	
	NO	No node switching is performed.	
Status		Displays the current status of the monitoring function.	
Status	ON	Monitoring is in progress.	
	OFF	Monitoring is stopped.	
Name		Displays the name of a virtual interface to be monitored.	
Mode	r	RIP mode	
	b	Fast switching/RIP mode	
	d	NIC switching mode (logical IP address takeover function)	
	e	NIC switching mode (physical IP address takeover function)	
Primary Target(status) Secondary Target(status)		Displays monitoring status in Primary/Secondary monitor-to IP address or a host name and parenthesis.	
		(ON)	Monitoring is in progress.
		(WAIT)	Waiting is in progress.
		(FAIL)	Monitoring failed (monitoring is stopped).
		(STOP)	Unused.
HUB-to-HUB status		Displays the status of HUB-to-HUB communication monitoring.	
HUB-to-HUB status	WAIT	HUB-to-HUB monitoring has stopped.	
	ACTIVE	HUB-to-HUB monitoring is operating.	
	FAIL	HUB-to-HUB monitoring has failed.	
	OFF	HUB-to-HUB monitoring is unused.	
	----	When RIP mode is being used.	

The following is the display format of monitoring status obtained when the -c option is specified.

```
# /opt/FJSVhanet/usr/sbin/dsppoll -c
     Node              VIP         POLL RIP        NIC         Status
+----------------+----------------+----+----+---------------+------+
 192.13.75.1      192.13.75.13      ON  ON   hahostA          ACTIVE
                                             192.13.73.12     FAIL
                                             192.13.72.19     ACTIVE
                                             192.13.73.19     ACTIVE
 hahostB          hahostC           ON  OFF  192.13.72.19     ACTIVE
                                             192.13.73.19     ACTIVE
                  hahostB           OFF OFF  192.13.72.19     ----
                                             192.13.73.19     ----
```

Item		**Explanation**
Node		Displays the name of a node to be monitored.
VIP		Displays the name of a virtual interface held by the monitored node.
POLL		Displays the operation mode of a virtual interface to be monitored.
POLL	ON	The monitoring function is enabled.
	OFF	The monitoring function is disabled.
RIP		Displays if or not a RIP packet is sent from the other device.
RIP	ON	RIP sending on (ON) from the other device.
	OFF	RIP sending off (OFF) from the other device.
NIC		Displays the hostname or IP address of a real interface to be monitored.
Status		Displays the monitoring status of a virtual interface.
Status	ACTIVE	Monitoring is in progress.
	FAIL	Monitoring failed (recover monitoring in progress).
	----	Monitoring is not yet performed.

[Related commands]

hanetpoll
hanetobserv

[Notes]

- If no option is specified, this command can be specified for a virtual interface in RIP mode (operation mode "r"), Fast switching/RIP mode (operation mode "b"), or NIC switching mode (operation mode "d" or "e").
- If the "-c" option is specified, this command can be specified for a virtual interface in GS/SURE linkage mode (operation mode "c").

[Examples]

(1) The following shows an example of displaying all the monitoring statuses properly defined using the hanetpoll command.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
```

(2) To display polling status of virtual interface sha0 for NIC Switching mode.

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

(3) When the monitoring information on GS/SURE linkage mode is displayed.

```
# /opt/FJSVhanet/usr/sbin/dsppoll -c
```

7.9 hanetnic Command

[Name]

hanetnic - Dynamic addition/deletion/switching of physical interfaces

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetnic command [args]

[Feature description]

The hanetnic command can add, delete, or switch physical interfaces to be used dynamically while the relevant virtual interface is active.

Command	Process outline	Authority
add	Adds physical interfaces	Super user
delete	Deletes physical interfaces	Super user
change	Changes physical interface used	Super user

When adding, deleting, or switching interfaces dynamically using this command, the virtual interface must be active.

Dynamic addition or deletion of a redundant physical interface is enabled even when a virtual interface of fast switching or a redundant physical interface of NIC switching is set for the network setting of the Solaris zone.

(1) add command

This command adds physical interfaces bundled by a virtual interface in Fast switching mode, RIP mode, Fast switching/RIP mode, and NIC switching mode dynamically. (Physical 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 (operation mode "t") or Fast switching/RIP mode (operation mode "b") 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)”.

The interface name specified in this option is an actual interface name (such as hmeX) for Fast switching, RIP and Fast switching/RIP modes. However, specification of the virtual interface (shaX) name used in operation mode “n” is required for GS/SURE linkage mode.

-f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic addition.)

(2) delete command

This command deletes physical interfaces bundled by a virtual interface in Fast switching mode dynamically (Physical 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:

```
/opt/FJSVhanet/usr/sbin/hanetnic delete -n devicename -i interface [-f]
```

-n devicename:

Specify a virtual interface name to which the physical interface to be deleted belongs. It is possible to specify only virtual interface names with Fast switching mode (operation mode "t") or Fast switching/RIP mode (operation mode "b").

-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.

The interface name specified in this option is actual interface name (such as hmeX) for Fast switching, RIP and Fast switching/RIP mode. However, specification of the virtual interface (shaX) name used in operation mode “n” is required for GS/SURE linkage mode.

-f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic deletion.)

(3) change command

This command changes physical interfaces used in a virtual interface in NIC switching mode to those of the standby system. The following is the format of the change command:

```
/opt/FJSVhanet/usr/sbin/hanetnic change -n devicename
```

-n devicename:

Specify the virtual interface name of the used physical interface to be changed. It is possible to specify only virtual interface names with NIC switching mode (operation mode "d" or “e”) specified.

[Notes]

- As for an actual interface to dynamically add for a virtual interface of Fast switching mode, RIP mode, and Fast switching/RIP mode (the operation mode is "t", "r", and "b"), be sure to define to use in TCP/IP before adding dynamically. (Check if or not there is /etc/hostname.interface file. If not, create it. Then execute "/usr/sbin/ifconfig a name of the actual interface plumb" command, and activate the interface.)

[Examples]

(1) add command

The following example adds hme0 to the bundled physical interfaces in the virtual interface sha0. It is assumed that sha0 has already been defined in Fast switching mode (operation mode "t") and hme0 has been deleted by using the "hanetnic delete" command.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i hme0
```

(2) delete command

The following example deletes hme1 from the bundled physical interfaces in the virtual interface sha0. It is assumed that sha0 has already been defined in Fast switching mode (operation mode "t").

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i hme1
```

(3) change command

The following example replaces physical interfaces used in the virtual interface sha0 with those of the standby system. It is assumed that sha0 has already been defined in NIC switching mode (operation mode "d").

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

7.10 strptl Command

[Name]

strptl - Starting the standby patrol

[Synopsis]

/opt/FJSVhanet/usr/sbin/strptl -n devicename1[,devicename2,...]

[Feature description]

The strptl command starts the standby patrol in NIC switching mode.

[Option]

You can specify the following option:

-n devicename1[,devicename2,...]

Specify the name of a virtual interface of the standby patrol to be started. You can specify more than one virtual interface by listing them delimited with a comma (,).

[Related commands]

stpptl

[Notes]

- The standby patrol is automatically started when the system is started up. Use this command to start the standby patrol manually after the system is started up.

[Examples]

The following shows an example of starting the standby patrol defined in a virtual interface (sha4).

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha4
```

7.11 stpptl Command

[Name]

stpptl - Stopping the standby patrol

[Synopsis]

/opt/FJSVhanet/usr/sbin/stpptl -n devicename1[,devicename2,...]

[Feature description]

The stpptl 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/stpptl -n sha4
```

7.12 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
```

7.13 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 "7.15 resethanet Command" for the detail of a resethanet command.
- The supported environment files for restoring the environment definition files with this command are the packages (FJSVhanet) with version 2.3 or later. The packages (FJSVhanet) prior to version 2.2 are not supported.

[Examples]

The following shows an example of restoring a file (/tmp/hanet20041129.bk) created using the backup command.

```
# /opt/FJSVhanet/usr/sbin/hanetrestore -f /tmp/hanet20041129.bk
```

7.14 hanethvrsc Command

[Name]

hanethvrsc - Sets the information of a virtual interface to register in the cluster resources.

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanethvrsc command [args]

[Feature description]

hanethvrsc command makes it possible to create/delete/display the information of a virtual interface to register in the resources of PRIMECLUSTER.

Command	Process outline	Authority
create	Creates virtual interface information	Super user
delete	Deletes virtual interface information	Super user
print	Displays virtual interface information	Super user

(1) create command

Creates the information of a virtual interface to register in the resources of PRIMECLUSTER. The information of a virtual interface is consisted of a logical virtual interface and a takeover IP address. It is possible to create up to 64 logical virtual interfaces. A logical number of a logical virtual interface (a number to add after ":") is automatically numbered from 65.

The following is the command format for creating a virtual interface information:

- When creating a virtual interface information

Fast switching mode:
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename -i {takeover-ipv4 | takeover-ipv6/prefix | takeover-ipv4,takeover-ipv6/prefix}

NIC switching mode:
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename

GS/SURE linkage mode:
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename [-i takeover-ipv4]

-n devicename:

Specify a name of the virtual interface for Fast switching, NIC switching or GS/SURE linkage mode created with hanetconfig command.
A multiple takeover IP can be applied to a single virtual interface name for Fast switching mode. For NIC switching mode and GS/SURE linkage mode (operation mode 'c'), one takeover IP can be applied against one virtual interface name.

-i takeover-ipv4[,takeover-ipv6/prefix]:

Specifies a host name or an IP address of a takeover IP. This option is necessary when a virtual interface to specify by -n option is Fast switching mode. Not necessary when NIC switching mode. In NIC switching mode, a value specified by -i option of hanetconfig create command is automatically set as a takeover IP. In GS/SURE linkage mode (operation mode 'c'), this option is omissible. When it omits, IP address set as virtual interface is automatically set up as takeover IP address.

(2) delete command

Deletes the information of a virtual interface from the cluster resources.

```
/opt/FJSVhanet/usr/sbin/hanethvrsc delete -n {devicename1[,devicename2,...] | all}
```

-n devicename:

Specifies a name of a logical virtual interface created by create command (shaXX:YY). However, it is not possible to delete while RMS is working.

(3) print command

Displays a list of the information of a virtual interface to register in the cluster resources.

```
/opt/FJSVhanet/usr/sbin/hanethvrsc print [-n devicename1[,devicename2,...]]
```

An example of a display is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
  ifname    takeover-ipv4    takeover-ipv6
+---------+---------------+-----------------------------------------------+
 sha1:65    takeover-ip1     -
 sha2:65    -                takeover-ip2
 sha3:65    192.168.70.1     fec0:1::123/64
```

Item	**Explanation**
ifname	A name of a logical virtual interface to register in the cluster resources is displayed.
takeover-ipv4	A host name or an IP address of a takeover IP (IPv4) to add to a logical virtual interface is displayed.
takeover-ipv6	A host name or an IP address of a takeover IP (IPv6) to add to a logical virtual interface is displayed.
'-'(hyphen)	Means that neither a hostname nor an IP address is set.

[Notes]

- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts and /etc/inet/ipnodes files. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.

[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 configuring GS/SURE linkage mode:
The following is an example of registering the virtual interface sha1 in the cluster resource.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1 -i 192.168.80.10
```

(2) delete command

An example of using create command when deleting a logical virtual interface sha1:65 from the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n sha1:65
```

(3) print command

An example of displaying a list of the information of a virtual interface to register to the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
```

7.15 resethanet Command

[Name]

resethanet - Initializes the information of virtual interface configuration and reactivates a Redundant Line Control function.

[Synopsis]

/opt/FJSVhanet/usr/sbin/resethanet -i | -s

[Feature description]

resethanet commands initializes the information of virtual interface configuration and reactivates a Redundant Line Control function. The initialized configuration information is as follows.

- The information of virtual interface configuration (the definition information set by hanetconfig command)
- The monitor-to information (the definition information set by hanetpoll command)

The parameters set by hanetpoll on command, hanetparam command, and hanetobserv command are not initialized.

[Option]

Specify the following options:

-i:

Specify to initialize the information of virtual interface configuration. Do not specify this option except to stop using a Redundant Line Control function during the operation, or to recreate the information of virtual interface configuration.

-s:

Specify to reactivate a Redundant Line Control function. This option validates changed content of the setting without rebooting a system when changed the information of virtual interface configuration.

(1) Initializing the configuration information

Initialize the configuration information of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/resethanet -i
```

-i:

Initializes the configuration information of a virtual interface and makes it the status of no definition. However, if even one virtual interface is registered as cluster resources in the corresponding system, it is not possible to initialize.

(2) Reactivating a Redundant Line Control function

Reactivates a Redundant Line Control function.

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

-s:

Reactivates a Redundant Line Control function. However, if RMS is activated at PRIMECLUSTER operation in a corresponding system, it is not possible to reactivate.

[Notes]

- When the configuration information is initialized with the command, it cannot be returned to the original state prior to initialization. Users are recommended to save the information using the hanetbackup command.
- If the Solaris zone is using the virtual interface, stop the Solaris zone then change the network setting before initializing the virtual interface configuration.
- When you execute this command, please stop RMS beforehand.

[Examples]

The following is an example of initialize the configuration information of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/resethanet -i
```

The following is an example of reactivates a Redundant Line Control Function.

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

Appendix A Messages and corrective actions

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

A.1 Messages Displayed by Redundant Line Control function

This section explains the meaning of, and action to take for each message output by Redundant Line Control function regarding such commands as the configuration commands and operation commands.

Each message has the following format:

[Output message]

1. A format for information messages and error output messages:

```
hanet: BBBCC DDDDD: EEEEE FFFFF
 (1)   (3)   (4)    (5)   (6)
```

2. A format for console output messages and internal information output messages:

```
hanet: AAAAA: BBBCC DDDDD: EEEEE FFFFF
 (1)   (2)    (3)   (4)    (5)   (6)
```

(1) Component name

Always begins with "hanet".

(2) Error Kind

Included in the console messages and internal information. AAAAA provides the following information:

ERROR:

Error message

WARNING:

Warning message

INFO:

Information message. It is only output when syslog ("3.2.3 syslog setup") is set.

TRACE:

Internal information

(3) Message number (Displayed in total five digits.)

Outputs an output message with a unique number. Not displayed when output an internal message.

The first three digits (BBB) indicate the message number.
The last two digits (CC) indicate the internal code.

(4) Outline of errors

The output information (DDDDD) is as follows. Not output when it is a console message.

information:

Means that an output message is the information.

warning:

Means that there is an error in the definition information (a process continues).

operation error:

Means that the executed command method has an error.

configuration error:

Means that there is an error in the definition information.

internal error:

Means that there is a fatal error.

(5) Error details

Message may be output as required.

(6) Others

The complimentary information (FFFFF) is occasionally output if necessary.

A.1.1 Information message (number 0)

Message number	Message	Meaning	Action
000	normal end.	Execution of the command was successfully completed.	None

A.1.2 Error output message (numbers 100 to 500)

The meaning of and response to each message output by Redundant Line Control function is listed below.

Message number 1xx

Message number	Message	Meaning	Action
101	command can be executed only with super-user.	Only a super-user can execute this command.	Please perform by a super-user authority.
102	this interface is already linked.	The specified virtual device has already been activated.	Execute the dsphanet command to make sure that the virtual interface is in the activated status.
105	invalid ip_address.	An invalid IP address is specified.	Specify the correct IP address for re-execution.
111	invalid parameter.	An invalid parameter is specified.	Read the appropriate command reference, and execute the command again.
112	invalid argument.	An invalid command argument was found.	Read the appropriate command reference, and execute the command again.
113	polling already active.	The router monitoring function has already been activated.	No action is required.
114	-r option value is invalid.	An invalid value is specified.	Read the appropriate command reference to get the correct value, and execute the command again.
115	-s -c option total value is invalid.	An invalid value is specified.	Specify the values (-s and -c) so that the product of the two values does not exceed 300, and execute the command again.
116	-s -c option value is invalid.	An invalid value is specified.	The values (-s and -c) must be selected from within a range of 1 to 300. Specify a number within the range for each value, and execute the command again.
117	polling already stopped.	The router monitoring function has already been deactivated.	No action is required.
118	interface is inactive.	The specified virtual interface has been	Execute the dsphanet command to check the

		deactivated.	status of the specified virtual interface.
119	interface is active.	The specified virtual interface has been activated.	Execute the dsphanet command to check the status of the specified virtual interface.
120	invalid device name.	An invalid virtual interface name is specified.	Specify the correct virtual interface name, and execute the command again.
121	directory not found.	The specified directory was not found.	Specify a directory name that already exists, and execute the command again.
122	backup file not found.	The specified backup file was not found.	Specify a backup file that already exists, and execute the command again.
123	invalid backup file.	The specified backup file is invalid.	Specify the backup file that was created by the hanetbackup command, and execute the command again.
124	not directory	Directory name was not found where directory was expected.	Specify a directory, and execute the command again.
125	interface is Cluster interface.	The specified interface is available in the cluster operation.	Specify an interface that is not being used in the cluster operation, and execute the command again.
126	shared resource is not found.	An invalid common resource is specified.	Specify a correct common resource name, and execute the command again.
127	invalid key	An invalid resource key is specified.	Specify a correct resource key, and execute the command again.
128	invalid logicalIP.	An invalid logical IP address is specified.	Specify a correct logical IP address, and execute the command again.
129	logicalIP is already defined.	The specified logical IP address has been specified in configuration information.	Specify a different logical IP address, and execute the command again.
130	logicalIP is not specified.	No logical IP address is specified.	Specify a logical IP address, and execute the command again.
131	primaryIF is not specified.	No primary interface is specified.	Specify a primary interface, and execute the command again.
132	invalid primaryIF.	An invalid primary interface is specified.	Specify a correct primary interface, and execute the command again.
133	physicalIP is not specified.	No physical IP address is	Specify a physical IP address for the interface,

		specified for the interface.	and execute the command again.
134	invalid physicalIP.	The physical IP address of the interface is invalid.	Specify a correct physical IP address, and execute the command again.
135	primary polling address is not specified.	No monitoring destination IP address is specified for the primary interface.	Specify a monitoring destination IP address for the primary interface, and execute the command again.
136	invalid primary polling address.	The monitoring destination IP address of the primary interface is invalid.	Specify a correct monitoring destination IP address, and execute the command again.
137	secondaryIF is not specified.	No secondary interface is specified.	Specify a secondary interface, and execute the command again.
138	invalid secondaryIF.	An invalid secondary interface is specified.	Specify a correct secondary interface, and execute the command again.
139	secondary polling address is not specified.	No monitoring destination IP address of the secondary interface is specified.	Specify a monitoring destination IP address of the secondary interface, and execute the command again.
140	invalid secondary polling address.	An invalid monitoring destination IP address is specified for the secondary interface.	Specify a correct monitoring destination IP address for the secondary interface, and execute the command again.
141	HUB-HUB polling flag is not specified.	Whether HUB-to-HUB communication monitoring is performed is not specified.	Specify whether to perform the HUB-to-HUB communication monitoring (ON or OFF), and execute the command again.
142	invalid HUB-HUB polling flag.	There is an error in the specification indicating whether HUB-to-HUB communication monitoring is performed.	Specify ON or OFF of the HUB-to-HUB communication monitoring, and execute the command again.
143	logicalIP is defined in physicalIP.	The IP address specified as a logical IP address overlaps the physical IP address.	Specify an IP address that is not specified in the virtual interface as the logical IP address, and execute the command again.
144	secondaryIF equal primaryIF.	The primary interface and the secondary interface are identical.	Specify different interfaces, and execute the command again.
145	interface is already defined in another set.	The specified interface is used in another operation set.	Specify an interface that is not used in other operation sets, and execute the command again.
146	interval is not specified.	No monitoring interval is specified.	Specify a monitoring interval, and execute the command again.

147	invalid interval specified.	The monitoring interval value is invalid.	Specify a correct monitoring interval, and execute the command again.
148	count is not specified.	No monitoring count is specified.	Specify a monitoring count, and execute the command again.
149	invalid count specified.	The monitoring count value is invalid.	Specify a correct monitoring count, and execute the command again.
150	invalid argument.	An invalid option is specified.	Refer to the command reference, and execute the command again.
151	logicalIP is active.	The specified processing could not be performed because the transmission line monitoring of the specified operation set was operating.	Stop the transmission line monitoring, and execute the command again.
152	logicalIP is inactive.	The specified processing could not be performed because the transmission line monitoring of the specified operation set was stopped.	Start the transmission line monitoring, and execute the command again.
153	logicalIP is not defined.	The specified operation set is not defined.	Specify a correct operation set.
154	logicalIP is registered to cluster resource.	The specified operation set is registered as a cluster resource.	Delete the operation set from the cluster resources.
155	invalid ping on/off.	HUB-to-HUB communication monitoring information specified in the operation set information is invalid.	Specify correct operation set information.
156	secondaryIF is not defined.	Because the secondary interface is not specified, interfaces cannot be switched.	Specify an operation set in which the secondary interface is defined.
157	product of interval and time should be less than 300.	The detection time (product of the monitoring interval and monitoring count) of line failure is too large.	Specify the monitoring interval and monitoring count so that their product does not exceed 300 seconds.
158	invalid interface count(max 32)	The maximum number of real interfaces that a virtual interface can bundle in GS/SURE linkage mode is exceeded (maximum 32).	Reduce the number of bundled real interfaces, and execute the command again.
159	MAC address is already defined.	The specified MAC address has already been specified.	Specify a different MAC address, and execute the command again.
160	specified devicename could	The specified device does not support cluster	Specify an interface name that support cluster

	not support cluster.	operation.	operation, and execute the command again.
161	polling function is defined.	The monitoring function is specified.	Delete a monitoring function with the name of the corresponding virtual interface, and execute again.
162	invalid MAC address.	An invalid MAC address is specified.	Specify a correct MAC address, and execute the command again.
163	IP address or Hostname is already defined.	The specified IP address or host name has already been specified.	Specify a different IP address or host name, and execute the command again. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 169, 170
164	interface name is already defined.	The specified interface name has already been specified.	Specify a different interface, and execute the command again. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 166
165	invalid interface name.	An invalid interface name is specified.	Specify a correct interface name, and execute the command again. When the virtual interface is registered in cluster resource, please execute it again after stopping RMS.
166	invalid mode.	A virtual interface configured with invalid operation mode or incompatible operation mode was specified.	Specify a virtual interface configured with valid operation mode or compatible operation mode.
167	parent device name not found.	No virtual interface corresponding to the logical virtual interface was found.	Specify a correct logical virtual interface, and execute the command again.
168	invalid hostname.	Specified host name or defined host name does not exist in /etc/inet/hostsfile or /etc/inet/ipnodes file. Or, specified host name is invalid.	Check for the existing host name specified in the command argument or hostname specified in configuration settings for Redundant Line Control function, in /etc/inet/hosts or /etc/inet/ipnodes file. If the host name does not exit, 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. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 166
170	invalid physical interface name.	An invalid physical interface name is specified.	Specify the correct name of the physical interface (the name of the virtual interface when the mode is "p" or "q"), and execute again. When setting a standby patrol function, check that two physical interfaces are defined that configure a virtual interface to be monitored. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 164
171	trunking interface list is not specified.	No interface that operates in trunking mode is specified.	Specify an interface, and execute the command again.
172	mode p interface is defined.	A virtual interface in mode P is specified.	Delete the interface in mode P, and execute the command again.
173	mode c interface is actived.	An interface in mode C is activated.	Inactivate the interface in mode C, and execute the command again.
174	ifname is not defined in hanetconfig.	The specified virtual interface name is not specified in configuration information.	Create configuration information using the hanetconfig command, and execute the command again.
175	same polling address are specified.	Primary and Secondary interfaces specified the same monitor-to address.	Specify different monitoring destinations, and execute the command again.
176	polling target is not alive.	No response is received from the monitoring destination.	Check the monitoring destination, and execute the command again.

177	polling is active.	The monitoring function is operating.	Stop (OFF) the monitoring function using the hanetpoll command, and execute the command again.
178	invalid version.	An incorrect version is specified.	Specify the version of the backed up Redundant Line Control function, and execute the command again.
179	invalid virtual interface count(max 64).	The number of virtual interfaces of the communication target exceeded the maximum number (maximum 64).	Delete unnecessary definitions, and execute the command again.
180	mode q interface is defined.	An invalid option is specified.	Deactivate an interface of mode q and execute again.
181	invalid client count(max 128).	An invalid option is specified.	Execute the command again with a correct value.
182	-p option value is invalid.	An invalid option is specified.	See the command reference and execute the command again with a correct value.
183	-b option value is invalid.	An invalid option is specified.	See the command reference and execute the command again with a correct value.
184	shared resource can not be specified.	An invalid option is specified.	See the command reference and execute the command again with a correct value.
185	function is already defined by another.	An invalid option is specified.	Check the configuration information again, delete unnecessary definitions, and execute again.
186	could not get information.	Communication between command-daemon failed.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
187	could not delete last 1 NIC.	It is not possible to delete if a using actual interface is only one when deleting dynamically an actual interface.	After stopped a virtual interface to process, delete or change the specified actual interface. When changing a definition of a virtual interface, delete or change a definition with hanetconfig command.
188	number of physical interface is already maximum.	The number of the physical interfaces that configures the specified virtual interface has reached the maximum number possible to bundle. Therefore, it is not possible to add an actual interface	Review the number of the physical interfaces that configures a virtual interface, and change a definition using a hanetconfig command if necessary.

		dynamically.	
189	invalid network address.	The specified network address is invalid.	Check if or not the specified network address matches with that of a virtual interface network using hanetconfig print command. Specify a correct network address again.
190	virtual gateway function is defined.	A virtual gateway function is already set.	Delete a virtual gateway function with the name of the corresponding virtual interface, then execute again.
191	StandbyIP address function is defined.	A function to specify a standby IP address is already set.	Delete a function to specify a standby IP address with the name of the corresponding virtual interface, and execute again.
192	resource monitor process for virtual interface is running.	A resource monitor for the virtual interface is working.	Execute hvshut command provided by a cluster system, halt a resource monitor, and execute again.
193	Specified interface is already linked to IP.	The IP address is already assigned to the specified interface.	Check if or not there is /etc/hostname.interface file. If exists, change a name or delete it. After executed “/usr/sbin/ifconfig interface name unplumb” command, execute the command again.
194	Specified interface is not bundled by a virtual interface.	The specified interface is not defined as the one to configure a virtual interface.	Check the interface that configures a virtual interface using hanetconfig print command. Specify an interface name displayed in the Interface List, and execute the command again. In addition, when you add the interface which does not exist on a definition, please specify "-f" option of the hanetnic add command, and execute the command again.
195	Standby patrol function could not started.	It is not possible to execute a standby patrol function.	Check that the system has already recognized all physical interfaces that configure a virtual interface to be monitored by a standby patrol function, and execute again.
196	Standby patrol function is defined.	A standby patrol function is already set.	Delete a standby patrol function of the corresponding virtual interface name, and execute again.
197	specified physical interface is	Activation of the specified physical interface is	Using dsphanet command, check that the specified

	already unlinked.	already deleted.	physical interface is not used yet.
198	address family of takeover IP address incompatible.	The specified address form of a takeover IP address (an address family) is not compatible with that of a setting virtual interface.	Make an address form of a takeover IP address compatible with that of a setting virtual interface and execute again.
199	invalid takeover IP address.	The specified takeover IP address is invalid.	Check a value of the specified takeover IP address and execute again.
200	invalid hostname or prefix value.	The specified host name or prefix value is invalid.	Check the specified host name or prefix value and execute again.
201	dual stack interface can not be specified.	It is not possible to specify a virtual interface of dual stack configuration.	Delete a definition of the corresponding virtual interface and define newly.
202	address family of polling IP address incompatible.	The specified address form of a monitor-to IP address (an address family) is not compatible with that of a setting virtual interface.	Make an address form of a monitor-to IP address compatible with that of a setting virtual interface and execute again.
203	interfaces defined as cluster resources still exist.	One or more virtual interfaces registered as cluster resources exist.	Delete the cluster resources and execute the command again.
204	interface defined as cluster resource is still active.	A virtual interface is active as cluster resources.	Stop RMS and execute again.
205	mode can't be changed for dual stack interface.	Mode can’t be changed if the virtual IF is a dual stack.	Temporary delete the configuration information of the virtual interface and reconfigure.
206	mode can't be changed for IPv6 interface.	Mode cannot be changed if the virtual IF is IPv6.	Temporary delete the configuration information of the virtual interface and reconfigure.
207	order of physical interface is different or invalid physical interface name.	Order of the interfaces is incorrect or the name of the interface is invalid.	Check the contents of the interface and retry.
208	configuration is not defined.	Valid configuration information or monitoring target's information is not configured.	Configure the valid configuration information or monitoring target's information.
209	specified address family is not defined.	The specified address type (address family) of the virtual interface is undefined.	Ensure the specified address matches the address format of configured virtual interface.
210	invalid address family.	The specified address type (address family) does not match the address type of the virtual interface.	Ensure the specified address matches the address format of configured virtual interface.
211	invalid MAC	The specified MAC	Specify a MAC address

	address(multicast or broadcast).	address is invalid.	other than a multicast address or broadcast address.
212	polling attribute of specified devicename cannot be changed individually.	The monitoring information of the virtual interface cannot be changed individually.	Specify the monitoring configuration value as changeable virtual interface that can be specified individually.
213	invalid interface name.(same physical interface)	Tagged VLAN interface created on the same physical interface was specified over the same physical interface.	Check the specified operation mode and tagged VLAN name. Then, retry the operation.
214	invalid interface name.(VLAN-ID is the same)	Identical logical device number of tagged VLAN interface is assigned.	Check the specified operation mode and tagged VLAN name. Then, retry the operation.
215	invalid interface name.(VLAN-ID different)	Disparate logical device number of tagged VLAN interface is assigned.	Check the specified operation mode and tagged VLAN name. Then, retry the operation.
216	When polling address is one, HUB-HUB polling flag must be OFF.	When polling address is one, HUB-HUB polling flag must be set OFF.	Set two polling targets or set the flag OFF, then retry the operation.
217	specified physical interface is inactive.	The specified physical interface is inactive.	Ensure the hostname configuration file (/etc/hostname.interface) for the physical interface exists. If it does no exist, create a new configuration file including physical IP address or hostname and then reboot the system After rebooting the system, execute the command. If the above file exists, run the following command: /usr/sbin/ifconfig [interface name] plumb [physical IP address] netmask + broadcast + up Then, execute the command again.
218	bundled interface does not exist.	A virtual interface bundling physical interface does not exist or a tagged VLAN interface does not exist.	Ensure virtual interface bundling physical interface or a tagged VLAN interface exists. Then re-execute the command.
219	invalid interface name.(physical interface is overlapped)	Specified Tagged VLAN interface is overlapped with part of physical interface or Tagged VLAN interfaces which belongs other virtual interface.	Specify un-overlapped or completely corresponding Tagged VLAN interfaces with other virtual interface.
220	interface is used in zones.	The virtual interface is used in the non-global zone.	Stop the non-global zone then execute the command again.
221	failed to inactivate virtual	Deactivation of the virtual	Stop the non-global zone

	interface.	interface failed.	then execute the command again. If the symptom still remains the same, collect troubleshooting information of the redundant line control then contact your Fujitsu system engineers.
222	invalid interface name.(unusable combination)	The physical interface name specified is invalid.	Check that the tagged VLAN interface is unmixed with the physical interface then execute the command again.
223	failed to activate interface.	Failed to activate a interface.	Activation of the interface failed because the same IP address was specified more than once or system resources are insufficient. Check the interface by executing the /usr/sbin/ifconfig command. If the symptom still remains the same, collect troubleshooting information of the redundant line control then contact your Fujitsu system engineers.

Message number 3xx

Message number	Message	Meaning	Action
301	could not open configuration file.	Failed to open the configuration information file.	Check whether the creation of configuration information has been completed.
302	invalid interface name.	An invalid virtual interface name was found in configuration information.	Review the configuration information.
303	hostname is not specified.	The host name is not specified in the configuration information.	Review the configuration information.
304	invalid hostname.	An invalid host name is specified in configuration information.	Review the configuration information.
305	trunking interface list is not specified.	The bundled physical interface is not specified in configuration information.	Review the configuration information.
306	invalid interface count(max 8).	The number of physical interfaces to be bundled exceeds the preset value.	Specify 8 or fewer physical interfaces as the number of interfaces to be bundled.
307	interface name is already defined.	The virtual interface name you want to specify has already been defined in the configuration information.	Specify a virtual interface so that it does not conflict with the other interfaces in the configuration information, and execute the command again.
308	physical interface name is already defined.	The physical interface name that you want to bundle in a virtual interface has already defined.	Review the configuration information.
309	interface address is already defined.	The same IP address is specified for more than one virtual interface.	Review the configuration information.
310	invalid physical interface name.	An invalid physical interface name is specified in the configuration information.	Review the configuration information.
311	invalid file format.	An invalid file format was found in configuration information.	Execute the check command for the configuration information, and take the appropriate action according to the output message.
312	parent device name not found.	The configuration information does not contain the virtual interface with the logical virtual interface.	Review the configuration information.
313	invalid mode.	An invalid operation mode is specified in the configuration information.	Review the configuration information.
314	target is not defined.	The destination	Review the destination

		information for monitoring does not contain the address information of the monitoring 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 address are specified.	Primary/Secondary interfaces specified the same monitor-to address.	Review the destination information for monitoring.
317	interface name is not defined.	The virtual interface name is not specified in the destination information for monitoring.	Review the destination information for monitoring.
318	invalid device count(max 64).	The number of specified virtual interfaces exceeds 64.	Review the configuration information or destination information for monitoring.
319	Invalid logical device count(max 63).	The number of specified logical virtual interfaces exceeds 63 (i.e., the maximum number for one virtual interface).	Review the configuration information.
320	Configuration is invalid.	The configuration information contains invalid data.	Review the configuration information.
321	Configuration is not defined.	Failed to find valid configuration information or destination information for monitoring.	Define the settings for the configuration information or destination information for monitoring.
322	invalid define count(max 64).	The total of defined virtual interfaces and defined logical virtual interfaces exceeds 64 (i.e., the maximum number for definition).	Review the configuration information.
323	LogicalIP is already max.	The number of logical IP addresses exceeded the maximum defined number.	Review the configuration information.
324	current configuration is invalid.	No operation set can be created because the definition of the created operation set contains invalid information.	Review the operation set information.
325	invalid ping on/off.	ON/OFF information for monitoring is not specified in the operation set information.	Review the operation set information.
326	invalid logicalIP.	The logical IP address is invalid.	Review the configuration information.
327	LogicalIP is already defined.	The logical IP address has already been specified.	Review the configuration information.

328	logicalIP not found.	The logical IP address was not found.	Review the configuration information.
329	primaryIF not found.	The primary interface was not found.	Review the configuration information.
330	invalid primaryIF.	The primary interface is invalid.	Review the configuration information.
331	physicalIP not found.	The physical IP address was not found.	Review the configuration information.
332	invalid physicalIP.	The physical IP address is invalid.	Review the configuration information.
333	primary polling address not found.	No monitoring destination address of the primary interface was found.	Review the monitoring destination information and configuration information.
334	invalid primary polling address.	The monitoring destination address of the primary interface is invalid.	Review the monitoring destination information and configuration information.
335	invalid secondaryIF.	The secondary interface is invalid.	Review the configuration information.
336	secondary polling address not found.	No monitoring destination address of the secondary interface was found.	Review the monitoring destination information and configuration information.
337	invalid secondary polling address.	The monitoring destination address of the secondary interface is invalid.	Review the monitoring destination information and configuration information.
338	HUB-HUB polling flag not found.	Whether HUB-to-HUB communication monitoring is performed is not specified.	Review the monitoring destination information and configuration information.
339	logicalIP equal physicalIP.	The same value is specified as the logical IP address and physical IP address.	Review the configuration information.
340	secondaryIF equal primaryIF.	The same value is specified as the primary interface and secondary interface.	Review the monitoring destination information and configuration information.
341	interface is already defined in another set.	An interface used in another operation set is specified.	Review the configuration information.
342	invalid HUB-HUB poll on/off.	There is an error in the specification indicating whether HUB-to-HUB communication monitoring is performed.	Review the monitoring destination information and configuration information.
343	physicalIP is already defined in another set.	A logical IP address used in another operation set is specified.	Review the configuration information.
344	polling information is different.	Different information is specified in the operation set sharing a physical interface.	Review the operation set information.

345	cluster configuration is incomplete.	The transmission line monitoring cannot be started because the cluster system settings are incomplete.	Review the setting of a cluster system, and reboot a machine.
346	invalid client count.	The number of the clients is improper.	Execute the command again with the correct number of the clients.
347	client address is already defined.	Already defined the specified client address.	See the client definition information, specify an address not redundant, and execute again.
348	invalid client address.	The specified client address is improper.	Check the client address and execute the command again.
349	invalid PmgropeID.	The PM group ID is improper.	Check the PM group ID and execute the command again.
350	invalid network address.	The specified network address is improper.	Check the network address and execute the command again.
351	observe information is not defined.	Not yet defined the monitoring item information.	Define the monitoring item information by hanetobserv command.
352	in.routed is not started.	Not yet activated a routing daemon (in.routed).	Change a system definition (check if or not there is /etc/defaultrouter file, change a name or delete it if exists) to activate a routing daemon (in.routed) and reboot the system.
353	invalid prefix value	A prefix value is invalid.	Check the specified IP address and previx value.
354	interface is specified redundantly.	Redundancy was found in the specified virtual interface. The redundancy will be ignored.	Specify the valid virtual interface and re-execute the command again.
356	could not get polling information.	Failed to obtain polling information.	Configure the polling information and re-execute the command. If the same error occurs after re-executing the command, then collect appropriate logs for Redundant Line Control function and contact our system engineers with the reported error message.
357	different network addresses are inappropriate.	The network addresses assigned between the interfaces do not match.	Review the assigned IP address (hostname) and network mask (prefix length). The network addresses between the interfaces must be the same network address. Assign the same network

			address between the interfaces.
358	the same network addresses are inappropriate.	The network addresses assigned between the interfaces cannot be the same network address.	Review the assigned IP address (hostname) and network mask (prefix length). The network addresses between must use different network address. Assign the different network addresses between the interfaces.
360	takeover ip address is not defined.	A takeover IP address is not set.	Review the setting of a Redundant Line Control function and a cluster system.
361	virtual interface is not defined.	A virtual interface is not set.	Review the setting of a Redundant Line Control function and a cluster system.
363	IP address is already defined in zones.	The IP address specified is already set in the non-global zone.	Change the IP address in the non-global zone, or specify a different IP address.
364	interface name is defined in zones.	The virtual interface specified for the non-global zone is deleted.	Change the interface for the non-global zone.
365	secondaryIF is specified in zones.	The secondary interface specified is already defined in the non-global zone.	Change the interface for the non-global zone to the primary interface.

Message number 5xx

Message number	Message	Meaning	Action
501	socket() fail.	An error was found in the internal system call.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster system. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual of a cluster system as to the materials necessary for examining a cluster system.
502	ioctl(SIOCGIFCONF) fail.	An error was found in the internal system call.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster system. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual of a cluster system as to the materials necessary for examining a cluster system.
510	could not allocate memory.	An error was found in the internal system call.	Execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). 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 a Redundant Line Control function, and tell an error message to Fujitsu system

			engineer (SE).
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 a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
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 a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
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 a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
515	ioctl(SHAIOCSETPARAM) fail.	An error was found in the internal system call.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
516	ioctl(I_PUNLINK) fail.	An error was found in the internal system call.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
517	ioctl(SHAIOCGETLID) fail.	An error was found in the internal system call.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a

			Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
518	ioctl(I_PLINK) fail.	An error was found in the internal system call.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
519	ioctl(SHAIOCPLUMB) fail.	An error was found in the internal system call.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
525	ioctl(SHAIOCGETINFO) fail.	An error was found in the internal system call.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
538	total entry is negative value.	An unexpected error occurred during reading configuration information.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
539	ioctl(SHAIOCNODENAME) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake,

			execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
540	ioctl(SHAIOCIPADDR) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
541	ioctl(SHAIOCSAP) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
542	ioctl(SHAIOCDEBUG) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
543	ioctl(SHAIOCWATCHDOG) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
544	ioctl(SHAIOCDISCARD) fail.	An unexpected system	Check that there is no a

		call error occurred.	mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
545	ioctl(SHAIOCMESSAGE) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
546	unexpected error.	An unexpected system call error occurred.	Execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
547	ioctl(SIOCGIFFLAGS) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
548	ioctl(SIOCGIFNUM) fail.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
549	polling process is inactive.	An internal process was not executed.	Collect materials for examination of a

			Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
550	opendir failed.	An unexpected system call error occurred.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
551	semaphore lock failed.	An error was found in the internal system call.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
552	semaphore unlock failed.	An error was found in the internal system call.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
553	shared memory attach failed.	An error was found in the internal system call.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
554	shared memory dettach failed.	An error was found in the internal system call.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
555	IPC key generate failed.	An error was found in the internal system call.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
556	get semaphore failed.	An error was found in the internal system call.	The following system resources are required for a Redundant Line Control function: * semsys:seminfo_semmni (The maximum number of the semaphore identifiers) : One or greater * semsys:seminfo_semmns (The maximum number of the semaphores in a system) : One or greater If the values are not

			sufficient, edit the kernel parameter file (/etc/system) and add the required value to the original parameter value. If the problem continues to occur after correcting the kernel parameter values, then there is a possibility that the semaphore identifier for the Redundant Line Control function has already been used by another application. In such case, follow the procedure described bellow to use a different identifier: # cd /opt/FJSVhanet/etc/sbin # mv hanetctld hanetctld.org # cp hanetctld.org hanetctld # shutdown -y -i6 -g0 If the problem still remains even after the identifier has been changed, collect examination materials of a Redundant Line Control function and contact a Fujitsu SE.
557	get shared memory segment identifier failed.	An error was found in the internal system call.	The following system resources are required for a Redundant Line Control function: * shmsys:shminfo_shmmax (The maximum size of the shared memory segment) : 5120 or greater * shmsys:shminfo_shmmni (The maximum number of the shared memory segments) : two or greater If the values are not sufficient, edit the kernel parameter file (/etc/system) and add the required value to the original parameter value. Additionally, do not specify shmsys:shminfo_shmmin(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 has already been used by another application. In such case, follow the procedure described bellow to use a different identifier:

			# cd /opt/FJSVhanet/etc/sbin # mv hanetselect hanetselect.org # cp hanetselect.org hanetselect If the problem still remains even after the identifier has been changed, collect examination materials of a Redundant Line Control function and contact a Fujitsu SE.
558	control semaphore failed.	An error was found in the internal system call.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
559	internal error.	An internal error occurred.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
560	control shared memory failed.	An error was found in the internal system call.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
561	daemon process does not exist.	An internal error occurred.	If not rebooted after the installation, first reboot, then execute again. There is a possibility that the command of Redundant Line Control function was executed after Redundant Line Control function stops when this message is output at the time of shutting down. Please review the execution timing of the command by the user. Moreover, please confirm whether /etc/rc2.d/S32hanet and /etc/rc3.d/S99hanet exists when basic OS is Solaris 8 or Solaris 9. When these files do not exist, please reboot the system after making /etc/rc2.d/S32hanet as a symbolic link to /etc/init.d/hanet and making /etc/rc3.d/S99hanet as a symbolic link to /etc/init.d/hanet99. If the same message is output even after rebooted, collect materials for examination of a Redundant Line Control

			function, and tell Fujitsu system engineer (SE) an error message.
562	failed to alloc memory.	Failed to acquire memory.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
563	failed to activate logicalIP.	An internal error occurred.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
564	failed to inactivate logicalIP.	An internal error occurred.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
565	ioctl(SHAIOCPATROLL) fail.	An error was found in the internal system call.	Execute the command again. If the same error message is output, contact a Fujitsu system engineer (SE) about the error message.
566	ether_aton() fail.	An error was found in the internal system call.	Check that there is no a mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
567	ioctl(SIOCGIFADDR) fail.	An error occurred in the internally used system call.	Check there is no mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute the command again. If the same phenomenon still occurs, collect materials for examination of a Redundant Line Control function, and tell Fujitsu SE an error message.
568	ioctl(SIOCGIFNETMASK) fail.	An error occurred in the internally used system call.	Check there is no mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute the command again. If the same

			phenomenon still occurs, collect materials for examination of a Redundant Line Control function, and tell Fujitsu SE an error message.
569	could not communicate with daemon process.	Failed to communicate between a command and a daemon.	Ensure the system is running as multi-user mode. If the system is running as single user mode, change it to multi-user mode and re-execute the command. If this error occurs while running the system as multi-user mode, collect the error logs and contact our system engineer.
570	failed to get socket.	An error occurred in the internally used system call.	Collect materials for examination of a Redundant Line Control function, and tell Fujitsu SE an error message.
571	failed to send request.	An error occurred in the internally used system call.	Collect materials for examination of a Redundant Line Control function, and tell Fujitsu SE an error message.
572	failed to receive response.	An error occurred in the internally used system call.	Collect materials for examination of a Redundant Line Control function, and tell Fujitsu SE an error message.
573	request timeout.	An error occurred in the internally used system call.	Collect materials for examination of a Redundant Line Control function, and tell Fujitsu SE an error message.
574	failed to delete virtual interface.	Failed to delete a virtual interface.	Execute the command again. If the same phenomenon still occurs, collect the examination materials of a Redundant Line Control function and inform a Fujitsu SE about an error message.
575	failed to restart hanet.	Failed to reactivate a Redundant Line Control function.	Execute the command again. If the same phenomenon still occurs, collect the examination materials of a Redundant Line Control function and inform a Fujitsu SE about an error message.
576	failed to enable configuration.	An error has occurred while processing the configured values.	Restart the Redundant Line Control function; (/opt/FJSVhanet/usr/sbin/resethanet -s) and review the reflected configuration

			values. If the same error occurs after rebooting the system, then collect appropriate logs for Redundant Line Control function and contact our system engineers with the reported 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.

Message number 8xx

Message number	Message	Meaning	Action
800	line status changed: Link Down at TRUNKING mode (interface on devicename, target=host_name)	An error occurred in the communication with the remote host system (host_name) using the physical interface (interface) controlled by the virtual interface (devicename) that is operating in the Fast switching mode.	Check whether an error has occurred on the communication path to the remote host system.
	line status changed: Link Down at RIP mode (target=host_name)	An error occurred in the communication with the remote host system (host_name).	Check whether an error has occurred on the communication path to the remote host system.
801	line status changed: Link Up at TRUNKING mode (interface on devicename, target=host_name)	The communication with the remote host system (host_name) using the physical interface (interface) controlled by the virtual interface (devicename) is recovered.	No action is required.
	line status changed: Link Up at RIP mode (target=host_name)	The communication with the remote host system (host_name) is recovered.	No action is required.
802	file open failed.	Failed to open the file.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
803	file read failed.	Failed to read the file.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
804	pipe create failed.	Failed to create the internal communication pipe.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
805	internal error.	An internal error occurred.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).

806	cannot get my process id	Failed to obtain the local process ID.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
814	cannot up interface.	Failed to up the virtual interface.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
815	sha device open failed.	Failed to open the "sha" driver.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
816	ioctl(SHAIOCSETRSCMON) failed.	Failed to send the monitor start request.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
817	ClOpen failed.	The connection to the cluster failed.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster system. If there is no mistake, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual of a cluster system as to the materials necessary for examining a cluster system.
822	no data in cluster event.	No data was found in the cluster event.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster system. If there is no mistake, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual of a cluster system as to the materials necessary for examining a cluster system.
823	ClSetStat failed.	The cluster resource status could not be set.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster

			system. If there is no mistake, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual of a cluster system as to the materials necessary for examining a cluster system.
824	directory open failed.	Failed to open the directory.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
825	signal send failed.	Failed to send the signal.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
826	command can be executed only with super-user.	The execution-time authority is invalid.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
827	could not allocate memory.	Failed to obtain the memory.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
828	fork failed.	The fork () failed.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
829	child process execute failed.	Failed to generate the child process.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
830	getmsg failed.	Failed to receive the data from the "sha" driver.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
831	shared library address get failed.	Failed to obtain the shared library address.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system

			engineer (SE).
832	poll failed.	The poll () failed.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
833	ioctl(SHAIOCSETIPADDR) failed.	Failed to notify the IP address.	Collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
840	polling device name is not defined in configuration information. polling is not started.	The virtual interface name for router monitoring is not defined in the configuration information. Thus, the router monitoring function for this virtual interface cannot be enabled.	Define the virtual interface name for router monitoring in the configuration information. Then, activate the virtual interface and inactivate/activate the router monitoring function.
841	all polling device name is not defined in configuration information. polling is not started.	No virtual interface for router monitoring is defined in the configuration information. Thus, the router monitoring function cannot be enabled.	Define the virtual interface name for router monitoring in the configuration information. Then, activate the virtual interface and inactivate/activate the router monitoring function.
842	device mode is invalid. polling is not started.	The operation mode of a virtual interface for router monitoring is invalid. Thus, the router monitoring function for this virtual interface cannot be enabled.	The operation mode of the virtual interface for router monitoring is defined as Fast switching mode. In Fast switching mode, line monitoring with the router monitoring function cannot be performed. Delete from the monitoring destination information the virtual interfaces whose operation mode is Fast switching mode.
843	polling device is not specified. polling is not started.	No monitoring destination information is specified. Or specified monitoring destination information contains invalid an error. Thus, the router monitoring function cannot be enabled.	Specify the monitoring destination information. Or correct the error in the settings. Then, disable and enable the router monitoring function.
844	polling address is invalid. polling is not started.	The monitoring destination address or host name specified in the monitoring destination information is invalid. Thus, the router monitoring function cannot be enabled.	Correct the monitoring destination address specified in the monitoring destination information. Then, disable and enable the router monitoring function.
845	could not restart in.routed.	Failed to restart the routing daemon. The	Check that there is no mistake in the setting of a

		router monitoring function is stopped and cluster switching is performed.	system, a Redundant Line Control function, and a cluster system. If the same phenomenon occurs, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual as to the materials necessary for examining a cluster system.
846	could not restart in.rdisc.	Failed to restart the router discovery daemon. The router monitoring function is stopped and cluster switching is performed.	Check that there is no mistake in the setting of a system, a Redundant Line Control function, and a cluster system. If the same phenomenon occurrs, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual as to the materials necessary for examining a cluster system.
847	internal error retry over. polling stop.	A router monitoring internal error occurred. The router monitoring is stopped.	Check that there is no mistake in the setting of a system, a Redundant Line Control function, and a cluster system. If the same phenomenon occurrs, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error message to Fujitsu system engineer (SE). See the manual as to the materials necessary for examining a cluster system.
848	device is inactive. polling stop.	The virtual interface for router monitoring is not activated. The router monitoring function is disabled.	Activate the virtual interface. Then, inactivate and activate the router monitoring function. This message may be displayed when cluster switching occurs during cluster operation, but in this case, no action is needed.
849	poll fail retry over. polling stop.	The transmission line failed as many times as specified by the retry count consecutively. The router monitoring function is disabled.	Check the line failure. After checking the line recovery, inactivate and activate the router monitoring function.

850	cannot down interface.	Failed to inactivate the physical interface.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster system. If there is no mistake, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
851	primary polling failed. lip=logicalIP, target=pollip.	An error of path to the primary monitoring destination was detected in the initial check of the physical interface. LogicalIP: Logical IP Pollip: Monitoring destination IP	Check for any failure on the communication path to the monitoring destination.
852	secondry polling failed. lip=logicalIP, target=pollip.	An error of path to the secondary monitoring destination was detected in the initial check of the physical interface. LogicalIP: Logical IP, pollip: Monitoring destination IP	Check for any failure on the communication path to the monitoring destination.
853	phisical interface up failed.	Failed to activate a physical interface.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster system. If there is no mistake, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
854	logical interface up failed.	Failed to activate a logical interface.	Check that there is no mistake in the setting of a Redundant Line Control function and a cluster system. If there is no mistake, collect materials for examination of a Redundant Line Control function, and tell an error message to Fujitsu system engineer (SE).
855	cluster logical interface is not found.	The logical interface registered with the cluster was not found.	Check that there is no mistake in the setting of a system, a Redundant Line Control function, and a cluster system. If the same phenomenon occurrs, collect materials for examination of a Redundant Line Control function and a cluster system, and tell an error

			message to Fujitsu system engineer (SE). See the manual as to the materials necessary for examining a cluster system.
856	cluster configuration is incomplete.	The logical IP address cannot be activated because the cluster settings are incomplete.	Review the cluster system settings, and reboot the system
857	polling information is not defined.	Monitoring destination information is not defined.	Define monitoring destination information using the hanetpoll command.
858	observe information is not defined.	Monitoring destination information is not defined.	Define monitoring destination information using the hanetobserv command.
859	in.routed is not started.	Routing daemon is not started.	Please change a setup and reboot a system so that /usr/sbin/in.routed is started. (Please check whether a /etc/defaultrouter file exists. If exists, change a file name or delete. Furthermore, please change the file name of /usr/sbin/in.rdisc into /usr/sbin/in.rdisc.saved etc.)
870	polling status changed: Primary polling failed. (ifname,target=pollip)	Line monitoring on the primary side failed. ifname: Interface name, pollip: Monitoring destination address	Check for any failure on the communication path to the monitoring destination.
871	polling status changed: Secondary polling failed. (ifname,target=pollip)	Line monitoring on the secondary side failed. ifname: Interface name, pollip: Monitoring destination address	Check for any failure on the communication path to the monitoring destination. If monitoring stopped after checking the recovery of the communication path, make a router/HUB monitoring function invalid and valid using the hanetpoll command. If monitoring fails even though possible to communicate normally, tune the intervals and the number of the times of monitoring, and the time to wait for a linkup with the hanetpoll command.
872	polling status changed: PrimaryHUB to SecondaryHUB polling failed. (ifname,target=pollip)	HUB-to-HUB communication monitoring on the primary side failed. ifname: Interface name, pollip: Monitoring destination address	Check for any failure on the communication path to the monitoring destination.

873	polling status changed: SecondaryHUB to PrimaryHUB polling failed. (ifname,target=pollip)	HUB-to-HUB communication monitoring on the secondary side failed. ifname: Interface name, pollip: Monitoring destination address	Check for any failure on the communication path to the monitoring destination.
874	polling status changed: HUB repair (target=pollip)	Line failure in HUB-to-HUB communication monitoring was repaired. pollip: Monitoring destination address	No action is required.
875	standby interface failed.(ifname)	An error involving standby interface was detected in the standby patrol. ifname: Interface name	Check that there is no error in a transfer route of the standby side. When it takes long time to link up, occasionally a recovery message is output immediately after this message is output. In this case, a transfer route of the standby side is normal. Therefore, not necessary to deal with.
876	node status is noticed.(sourceip:status)	A node status change was notified from the remote system. sourceip: Source address, status: Notified status	Check the status of the source.
877	route error is noticed.(sourceip)	A communication path failure was notified from the remote system. sourceip: Source address	Check for any failure on the communication path to the source.
878	route error is detected.(target=IP)	A communication path failure was detected from the remote system. IP: Remote system address	Check for any failure on the communication path to the source.
879	message received from unknown host.(srcaddr)	A message was received from an unregistered remote system. srcaddr: Source address	Register the corresponding remote host using the hanetobserve command.
880	failed to send node down notice by time out. (dstip)	Node status notification failed due to timeout. dstip: Destination address	Check for any failure of the remote system and on the communication path to the remote system.
881	semaphore is broken. (errno)	Creates a semaphore again because it is deleted.	Not necessary to deal with.
882	shared memory is broken. (errno)	Creates a shared memory again because it is deleted.	Not necessary to deal with.
883	activation of a wrong interface has been detected. (ifname)	Since the interface was unjustly activated by the user, the state of an interface is restored. ifname: interface name	Check that the interface has been recovered correctly. In addition, when this message is displayed to the user operating nothing, please investigate the cause of the

			abnormality occurred.
884	unexpected interface deactivation has been detected. (ifname)	Since the interface was unjustly deactivated by the user, the state of an interface is restored. ifname: interface name	Check that the interface has been recovered correctly. In addition, when this message is displayed to the user operating nothing, please investigate the cause of the abnormality occurred.
885	standby interface recovered.(ifname)	It detected that the route by the side of standby was recovered by standby patrol. ifname: interface name of standby patrol	Not necessary to deal with.
886	recover from route error is noticed.(ifname)	The recovery was notified from the remote system. ifname: Interface name	Not necessary to deal with.
887	recover from route error is detected. (target=IP)	The recovery of the remote system was detected. IP: Remote system address	Not necessary to deal with.
888	interface is activated. (ifname)	The physical interface was activated. ifname: Interface name	Not necessary to deal with.
889	interface is inactivated. (ifname)	The physical interface was inactivated. ifname: Interface name	Not necessary to deal with.
890	logical IP address is activated. (logicalIP)	The logical IP address was activated. logicalIP: Logical IP	Not necessary to deal with.
891	logical IP address is inactivated. (logicalIP)	The logical IP address was inactivated. logicalIP: Logical IP	Not necessary to deal with.
892	logical virtual interface is activated. (ifname)	The logical virtual interface was activated. ifname: Interface name	Not necessary to deal with.
893	logical virtual interface is inactivated. (ifname)	The logical virtual interface was inactivated. ifname: Interface name	Not necessary to deal with.
894	virtual interface is activated. (ifname)	The virtual interface was activated. ifname: Interface name	Not necessary to deal with.
895	virtual interface is inactivated. (ifname)	The virtual interface was inactivated. ifname: Interface name	Not necessary to deal with.
896	path to standby interface is established. (ifname)	Monitoring by standby patrol started normally. Ifname: A name of a standby patrol interface.	Not necessary to deal with.
897	immediate exchange to primary interface is canceled. (ifname)	Restrained prompt failback to the primary interface by standby patrol. ifname: A name of an	Not necessary to deal with. When executing prompt failback, use a hanetpoll modify command and change the monitor-to

		interface. This message is output when the monitor-to information to set by a hanetpoll create command is other than HUB.	information to a host name or an IP address of HUB.
899	route to polling address is inconsistent.	The network address defined to virtual interface and monitoring target is not the same, or since inappropriate routing information was registered into routing table, the mistaken monitoring is performed.	Please correct, when you check monitoring target address and there is an error. When there is no error in monitoring target address, please check whether inappropriate routing information is registered into the routing table. When using tagged VLAN interface, please confirm whether a virtual interface is a setting of NIC switching mode (operation mode "d"). If the setting of a virtual interface is NIC switching mode (operation mode "e"), please change the setting of corresponding monitoring information.

Message number 9xx

Message number	Message	Meaning	Action
901	failed to takeover logical interface used in zone.	Takeover of the logical interface for the non-global zone failed.	The following causes are suspected: * The number of logical interfaces reaches the maximum. * The same IP address is used for two or more interfaces in the system. * The same IP address is used for the other node and IPv6.Check the network interface and network environment in the system.
902	logical interface of zone was added to a secondaryIF.	The logical interface for the non-global zone was added to the secondary interface.	The secondary interface is set to the network interface of the non-global zone. Changing the interface to the primary interface is highly recommended. However, this will not affect ongoing operations because the logical interface for the non-global zone will automatically be taken over to the primary interface.
903	succeeded in takeover logical interface used in zone.	The logical interface for the non-global zone was succeeded.	Not necessary to deal with.
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.

A.1.4 Internal information output messages (no message number)

The following describes the messages to output the internal information of Redundant Line Control function to /var/adm/messages, and their meaning.

Message number	Message	Meaning	Action
-	update cluster resource status.	To update the state of the cluster resources.	No action is required.
-	receive message from sha driver.	Received a message from an SHA driver.	No action is required.
-	receive event from cluster:	Received an event from the cluster management.	No action is required.
-	polling	To control a monitoring function.	No action is required.
-	in.routed killed.	To terminate an in.routed daemon process.	No action is required.
-	in.rdisc killed.	To terminate an in.rdisc daemon process.	No action is required.
-	child proc exit.	A monitoring process terminated.	No action is required.

A.1.5 DR connection script error output messages

In a DR connection script of a Redundant Line Control function, a message is output when not possible to continue communication by disconnecting the corresponding virtual interface and the actual interface due to a certain reason, or when failed to disconnect or connect detecting an error in the workings of a DR connection script. The messages displayed in a DR connection script of a Redundant Line Control function are as follows:

Code	Message	Meaning	Action
0001	When the DR processing is executed for this NIC, the communication is disconnected. The DR processing is stopped. devicename=XX interface=YY	When executed a DR process to an interface YY that a virtual interface XX bundles, the communication is disconnected. Stops the DR process.	Deactivate a virtual interface XX, delete a definition of a virtual interface XX, and execute a DR process again.
0002	The interface is Cluster interface. The DR processing is stopped. action=ZZ devicename=XX interface=YY	A virtual interface XX that bundles an interface YY is already registered as the cluster resource. Stops a DR process.	Delete a definition of the cluster environment and execute a DR process again.
0003	hanetnic command abnormal end. action=ZZ devicename=XX interface=YY	Ended abnormally by a hanetnic command (ZZ subcommand) while having a DR process to an interface YY that is bundled into a virtual interface XX.	Check that there is no mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a DR process again. If the same phenomenon occurs, tell an error message to Fujitsu system engineer (SE).
0004	strptl command abnormal end. devicename=XX interface=YY	Ended abnormally by an strptl command while executing a DR process to an interface YY that is bundled into a virtual interface XX.	Check that there is no mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a strptl command again. If the same phenomenon occurs, tell an error message to Fujitsu system engineer (SE).
0005	stpptl command abnormal end. devicename=XX interface=YY	Ended abnormally by an stpptl command while executing a DR process to an interface YY that is bundled into a virtual interface XX.	Check that there is no mistake in the setting of a Redundant Line Control function. After checked there is no mistake, execute a DR process again. If the same phenomenon occurs, tell an error message to Fujitsu system engineer (SE).

0006	hanetpoll on command abnormal end.	Ended abnormally by hanetpoll on command.	After processed DR, check that the settings of a Redundant Line Control function has no mistake, and execute hanetpoll on command. If an error occurred even after that, check how to deal with the displayed error in a manual and follow the instructions.
0007	hanetconfig modify command abnormal end. devicename=XX NIC_list=YY	While processing DR to the interface XX that is bundled into a virtual interface YY, ended abnormally by hanetconfig modify command.	Check that the settings of a Redundant Line Control function has no mistake. After checked there is no mistake, execute a DR process again. If the same phenomenon occurred even after that, tell Fujitsu SE an error message.
0008	Is the DR processing continued ?	Do you continue to process DR?	Input "YES" to continue, "NO" to end. Inputting "YES" into this message to continue DR processing is recommended.
0009	The interface is IPv6 interface. The DR processing is stopped. action=delete interface=YYYY	A virtual interface that uses an IPv6 address in an interface YYYY exists. Stops DR processing.	Delete the configuration information that uses an IPv6 address and execute the DR processing again.

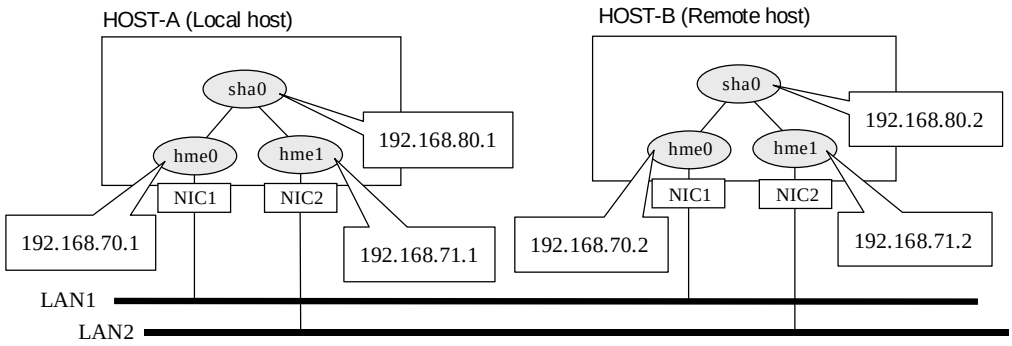
Appendix B Examples of configuring system environments

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.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

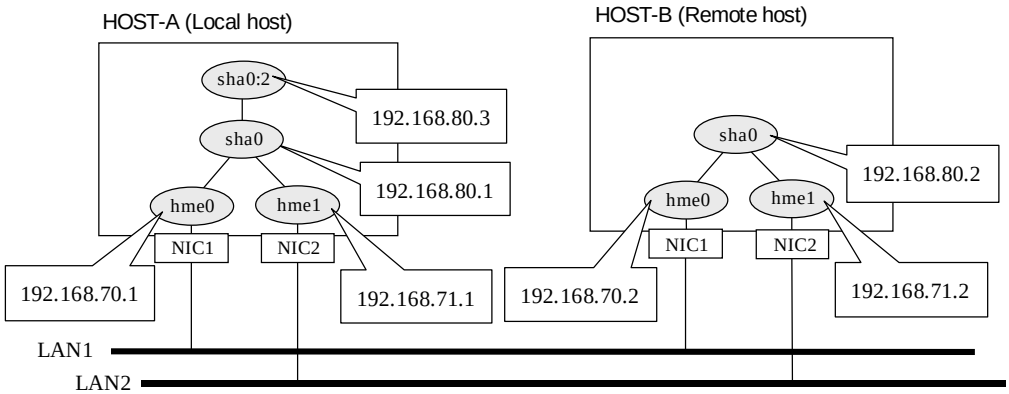
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.1.2 Example of the Single system in Logical virtual interface

This section describes an example configuration procedure of the network shown in the diagram below.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.80.3    hosta1   # HOST-A Logical virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1

4) Creation of logical virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3

5) Activation of virtual interface and logical virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

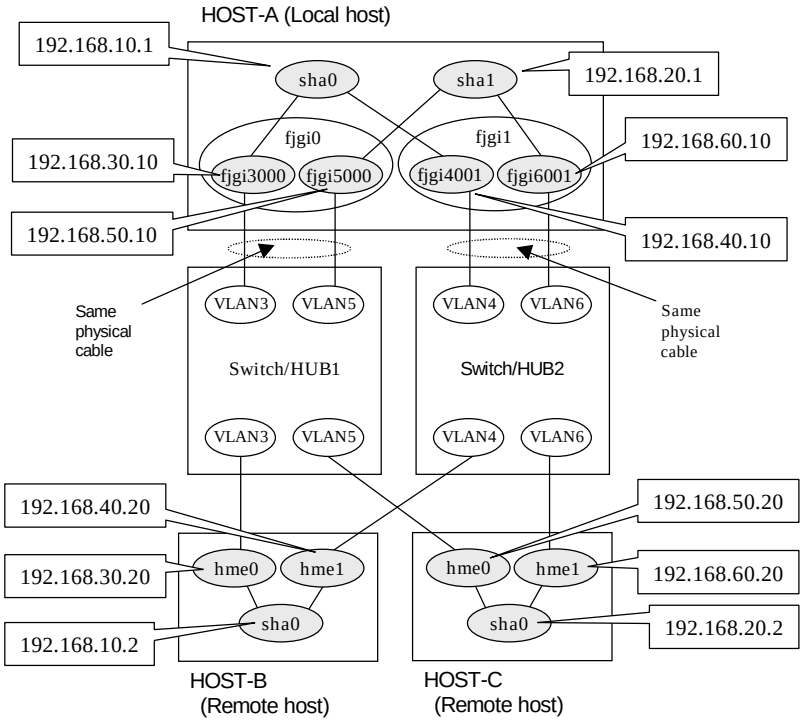
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.1.3 Configuring virtual interfaces with tagged VLAN

This section describes an example configuration procedure of the network shown in the diagram below.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.10.1    hosta1    # HOST-A Virtual IP
192.168.20.1    hosta2    # HOST-A Virtual IP
192.168.30.10   hosta3    # HOST-A Physical IP (Tagged VLAN interface)
192.168.40.10   hosta4    # HOST-A Physical IP (Tagged VLAN interface)
192.168.50.10   hosta5    # HOST-A Physical IP (Tagged VLAN interface)
192.168.60.10   hosta6    # HOST-A Physical IP (Tagged VLAN interface)
192.168.10.2    hostb1    # HOST-B Virtual IP
192.168.30.20   hostb3    # HOST-B Physical IP
192.168.40.20   hostb4    # HOST-B Physical IP
192.168.20.2    hostc2    # HOST-C Virtual IP
192.168.50.20   hostc5    # HOST-C Physical IP
192.168.60.20   hostc6    # HOST-C Physical IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi3000

```
hosta3
```

- Contents of /etc/hostname.fjgi4001

```
hosta4
```

- Contents of /etc/hostname.fjgi5000

```
hosta5
```

- Contents of /etc/hostname.fjgi6001

```
hosta6
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.10.0    255.255.255.0
192.168.20.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure fjgi3000, fjgi4001, fjgi5000 and fjgi6001 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t fjgi3000,fjgi4001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t fjgi5000,fjgi6001

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hostb3
```

- Contents of /etc/hostname.hme1

```
hostb4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hostc5
```

- Contents of /etc/hostname.hme1

```
hostc6
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

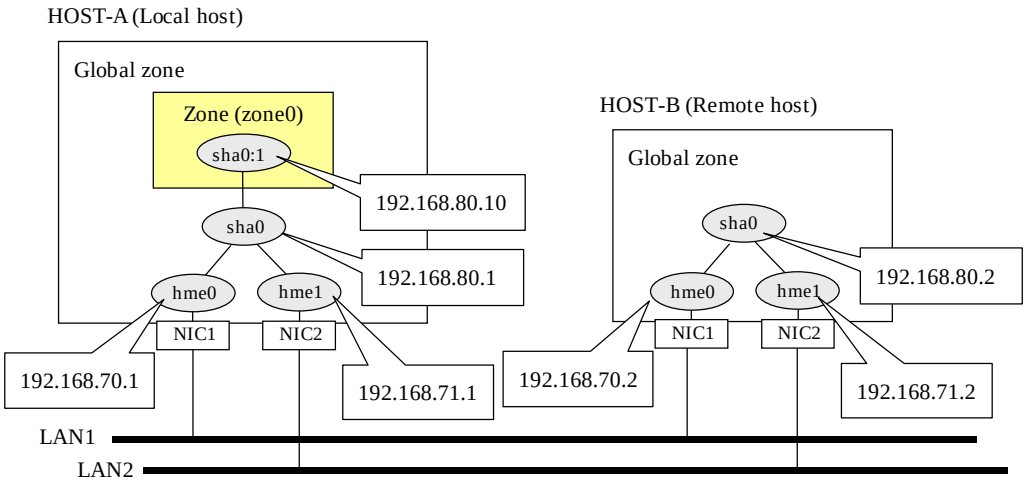
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.1.4 Network configuration in the Solaris container

This section describes an example configuration procedure of the network shown in the diagram below.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1     host11    # HOST-A Physical IP (1)
192.168.71.1     host12    # HOST-A Physical IP (2)
192.168.80.1     hosta     # HOST-A Virtual IP
192.168.70.2     host21    # HOST-B Physical IP (1)
192.168.71.2     host22    # HOST-B Physical IP (2)
192.168.80.2     hostb     # HOST-B Virtual IP
192.168.80.10    zone0      # zone0 Logical IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0     255.255.255.0
192.168.71.0     255.255.255.0
192.168.80.0     255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

5) Set up a zone

Set up a zone by executing the following command:

/usr/sbin/zonecfg -z zone0

5-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

5-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in fast switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.80.10/24
zonecfg:zone0:net> set physical=sha0
zonecfg:zone0:net> end
```

5-3) Check the above setting.

```
zonecfg:zone0> export
```

5-4) Check setup consistency.

```
zonecfg:zone0> verify
```

5-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

6) Install the zone

Install the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 install

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

7) Start up the zone

Start up the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 boot

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1

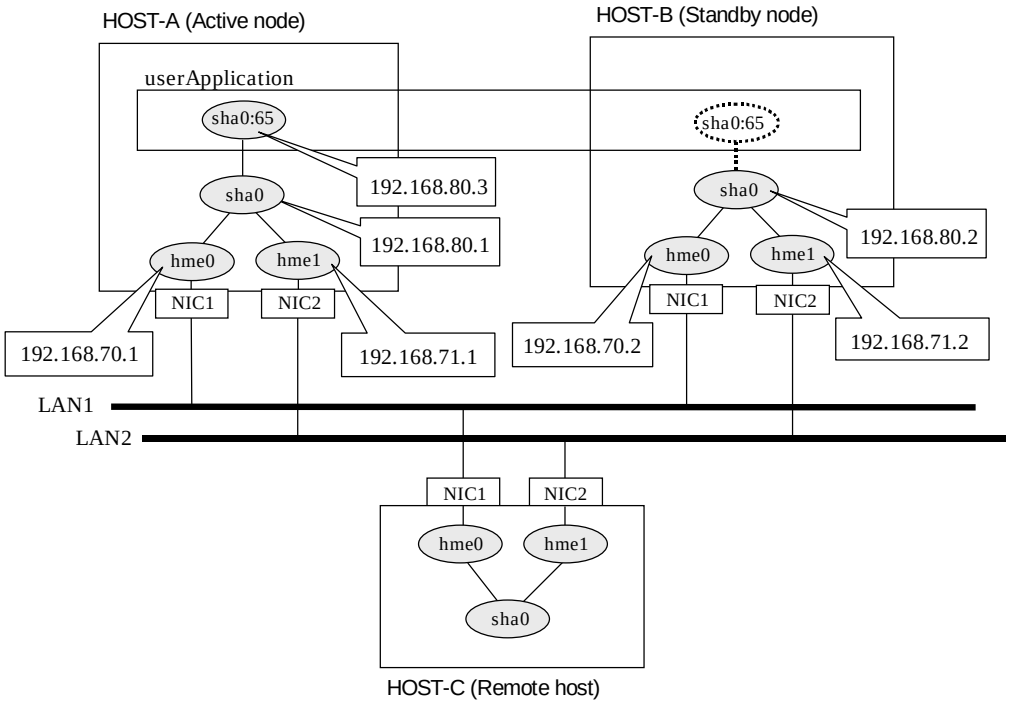
4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.1.5 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.80.3    hosta1   # Takeover virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resource, select the SysNode for HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.3”.

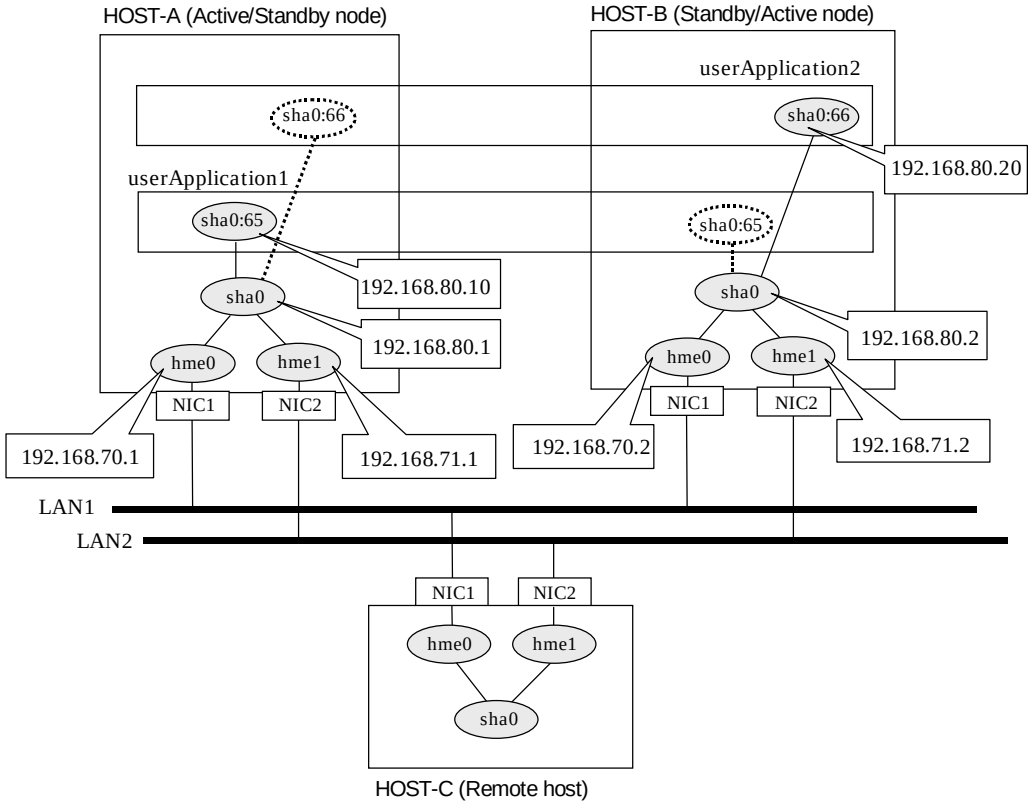
2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.1.6 Example of the Cluster system (Mutual Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1     host11   # HOST-A Physical IP (1)
192.168.71.1     host12   # HOST-A Physical IP (2)
192.168.80.1     hosta    # HOST-A Virtual IP
192.168.70.2     host21   # HOST-B Physical IP (1)
192.168.71.2     host22   # HOST-B Physical IP (2)
192.168.80.2     hostb    # HOST-B Virtual IP
192.168.80.10    hosta1   # Takeover virtual IP (1)
192.168.80.20    hostb1   # Takeover virtual IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.3” and “192.168.80.10”.

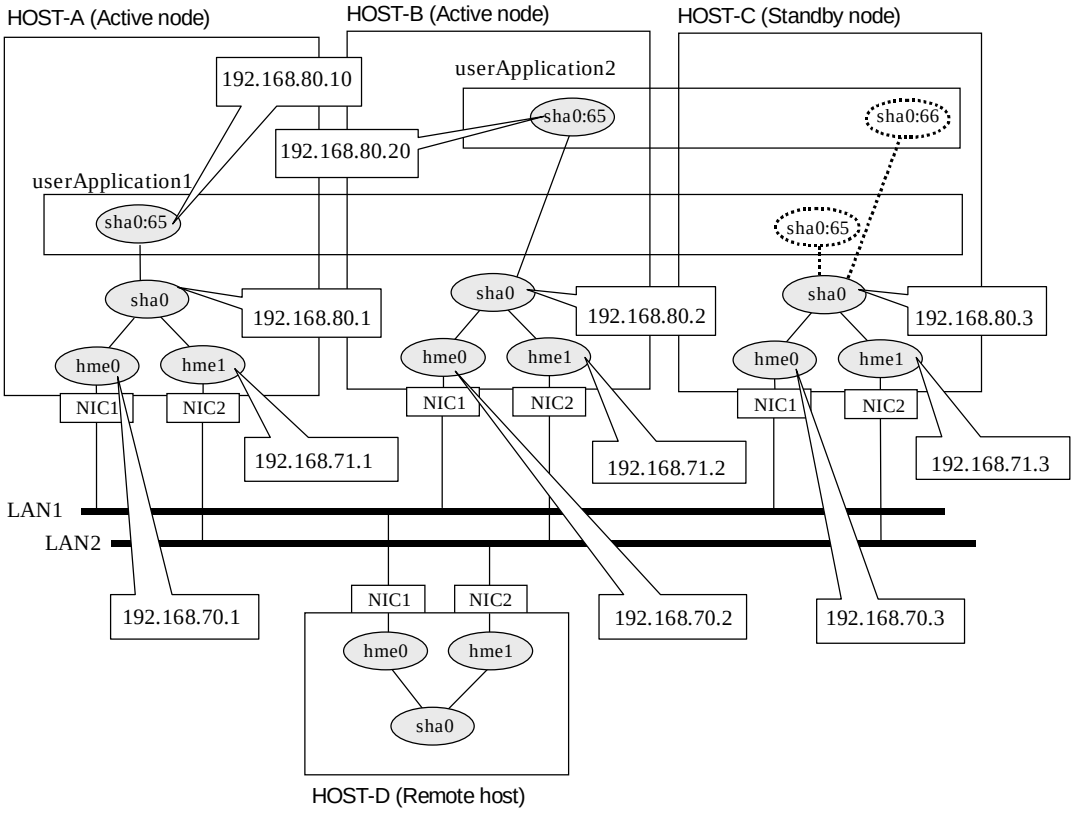
2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.1.7 Example of the Cluster system (N:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1     host11   # HOST-A Physical IP (1)
192.168.71.1     host12   # HOST-A Physical IP (2)
192.168.80.1     hosta    # HOST-A Virtual IP
192.168.70.2     host21   # HOST-B Physical IP (1)
192.168.71.2     host22   # HOST-B Physical IP (2)
192.168.80.2     hostb    # HOST-B Virtual IP
192.168.70.3     host31   # HOST-C Physical IP (1)
192.168.71.3     host32   # HOST-C Physical IP (2)
192.168.80.3     hostc    # HOST-C Virtual IP
192.168.80.10    hosta1   # Takeover virtual IP (1)
192.168.80.20    hostb1   # Takeover virtual IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host31
```

- Contents of /etc/hostname.hme1

```
host32
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of HOST-A, HOST-B, and HOST-C connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.3” and “192.168.80.10”.

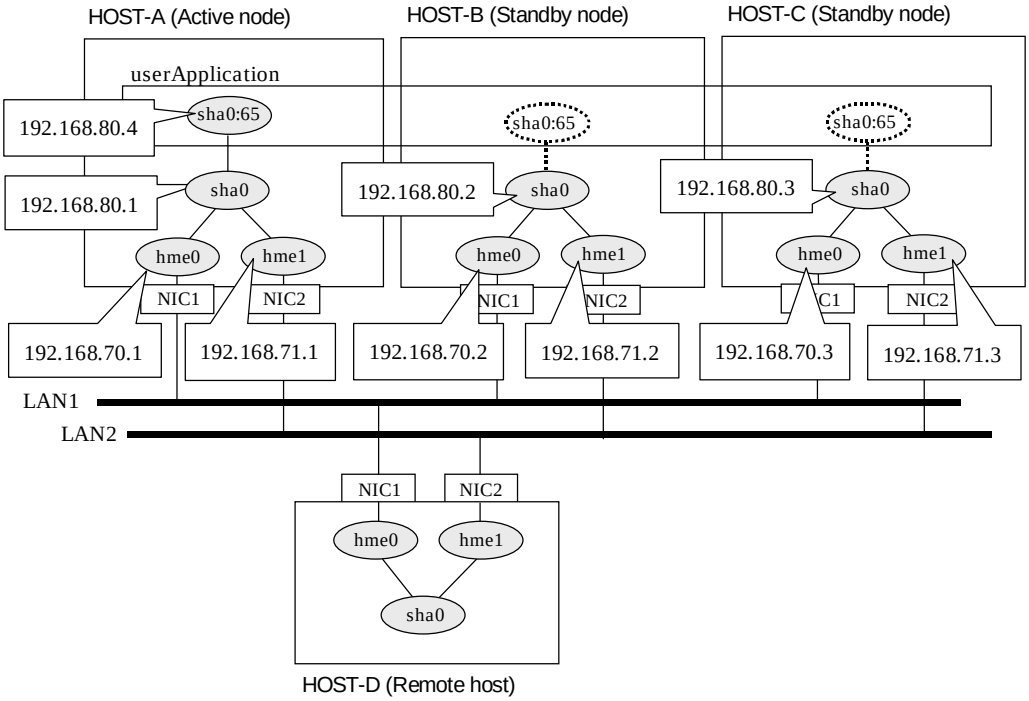
2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.1.8 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.70.3    host31   # HOST-C Physical IP (1)
192.168.71.3    host32   # HOST-C Physical IP (2)
192.168.80.3    hostc    # HOST-C Virtual IP
192.168.80.4    hosta1   # Takeover virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
```

```
192.168.80.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host31
```

- Contents of /etc/hostname.hme1

```
host32
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.4”.

2) Starting of userApplication

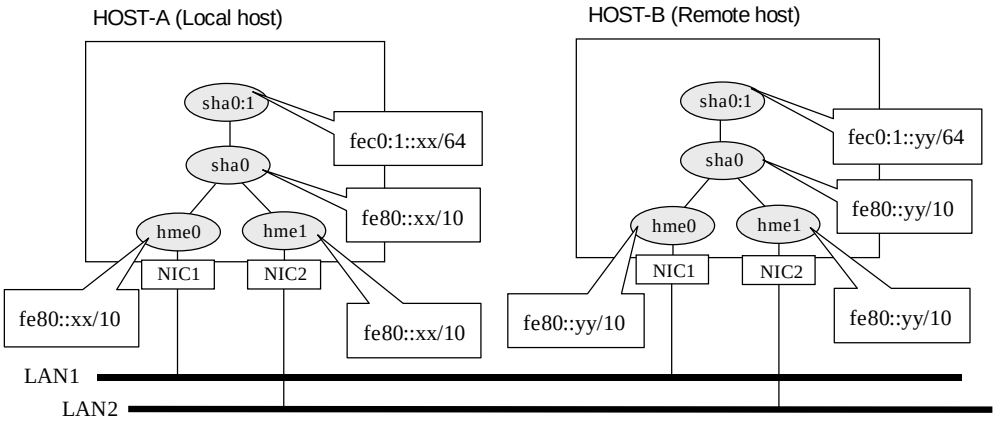
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2 Example of configuring Fast Switching mode (IPv6)

B.2.1 Example of the Single system

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

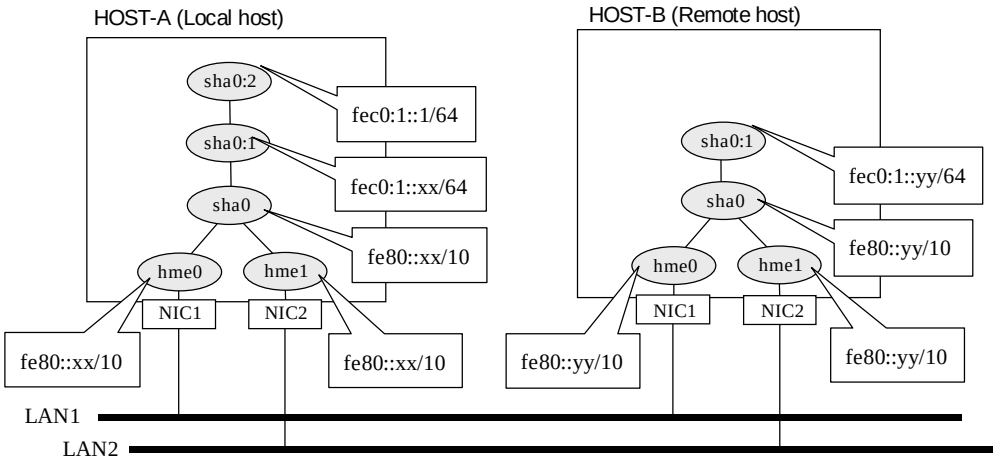
4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.2.2 Example of the Single system in Logical virtual interface

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1          v6hosta1     # Logical virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of logical virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0:2 -i fec0:1::1/64

5) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-2) Define logical virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

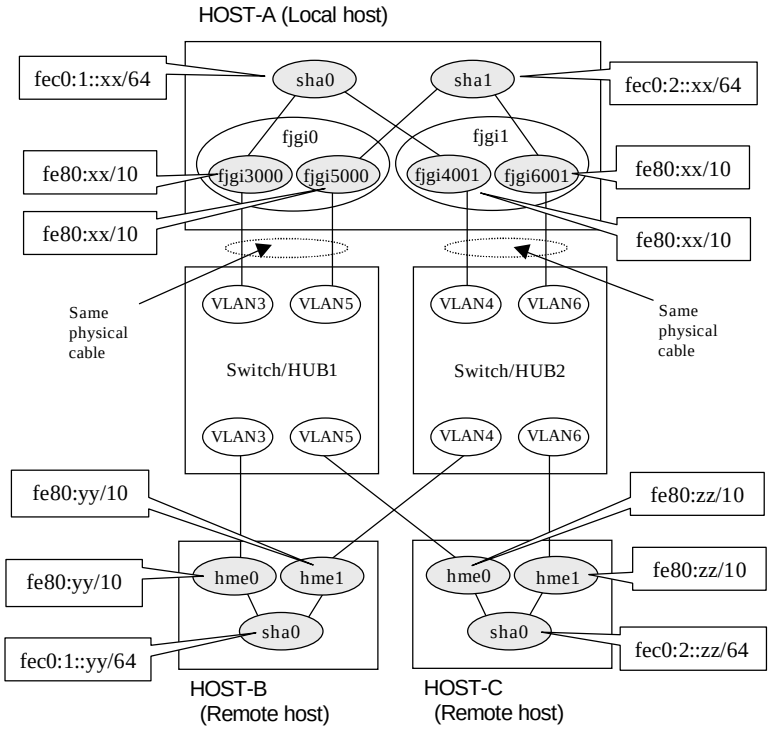
4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.2.3 Configuring virtual interfaces with tagged VLAN

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true   # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0               # sha0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 sha1               # sha1 sends Prefix "fec0:2::0/64".
```

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.fjgi3000,/etc/hostname6.fjgi4001,/etc/hostname6.fjgi5000 and /etc/hostname6.fjgi6001 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure fjgi3000, fjgi4001, fjgi5000 and fjgi6001 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi3000,fjgi4001

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m t -t fjgi5000,fjgi6001

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-C]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true   # Every interface sends a router advertisement.
prefix fec0:2::0/64 sha0               # sha0 sends Prefix "fec0:2::0/64".
```

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

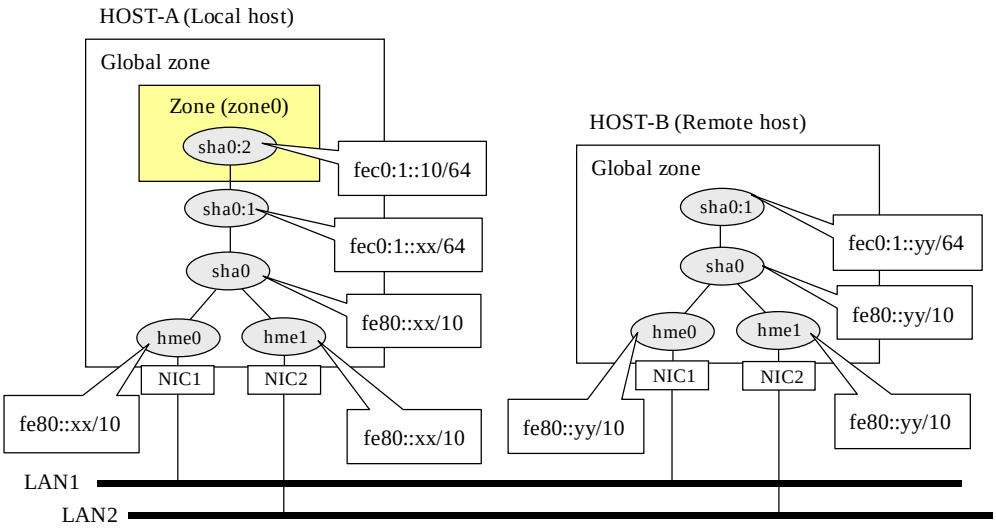
4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.2.4 Network configuration in the Solaris container

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

5) Set up a zone

Set up a zone by executing the following command:

/usr/sbin/zonecfg -z zone0

5-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

5-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in fast switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=sha0
zonecfg:zone0:net> end
```

The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.

5-3) Check the above setting.

```
zonecfg:zone0> export
```

5-4) Check setup consistency.

```
zonecfg:zone0> verify
```

5-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

6) Install the zone

Install the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 install

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

7) Start up the zone

Start up the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 boot

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.2.5 Example of the Cluster system (1:1 Standby)

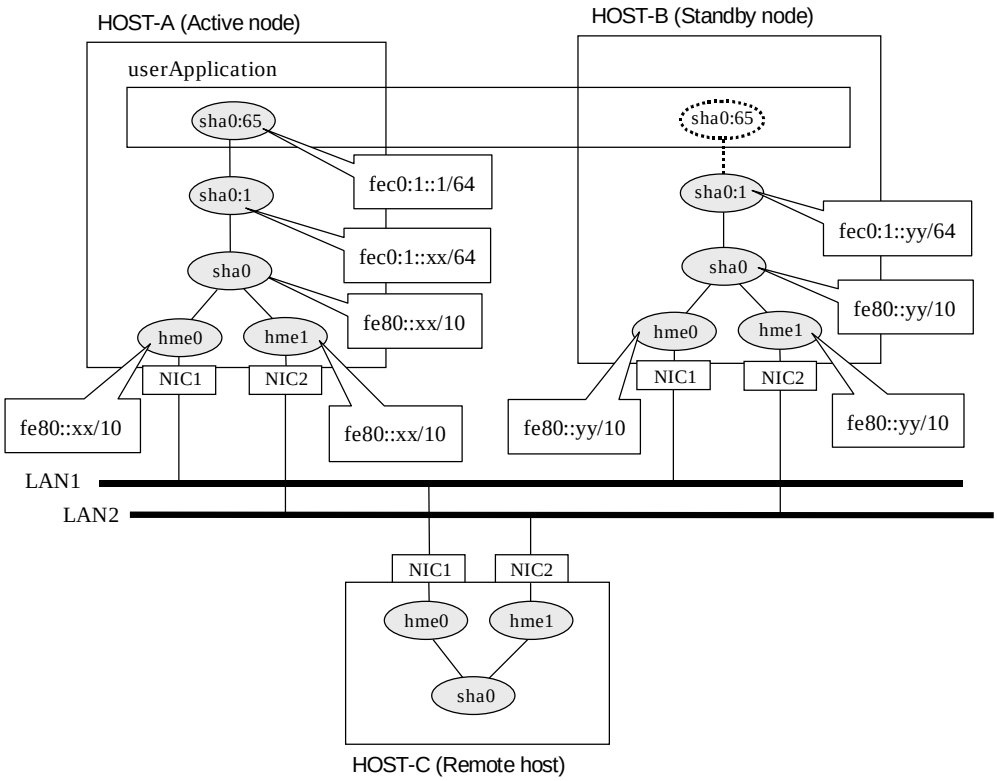
This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1          v6hosta1     # Takeover virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resource, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::1”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2.6 Example of the Cluster system (Mutual standby)

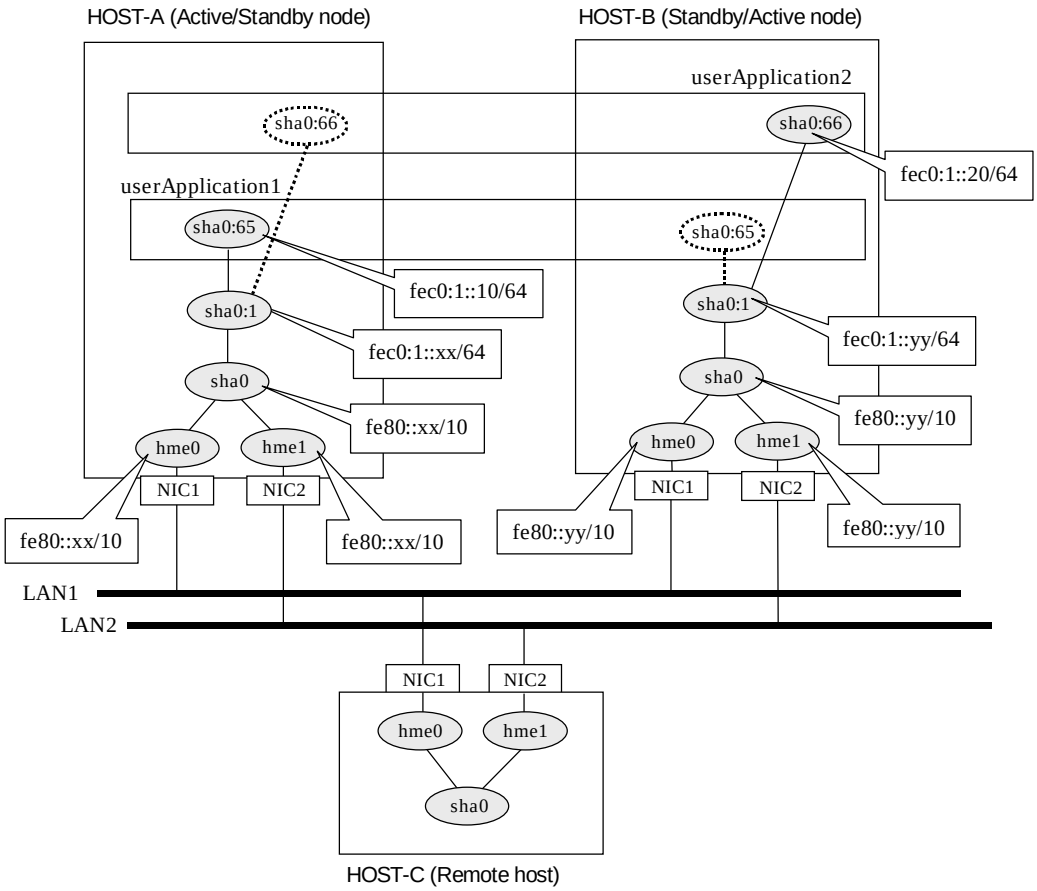
This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10      v6hosta1    # Takeover virtual IP (1)
fec0:1::20      v6hostb1    # Takeover virtual IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::10” and “fec0:1::20”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2.7 Example of the Cluster system (N:1 Standby)

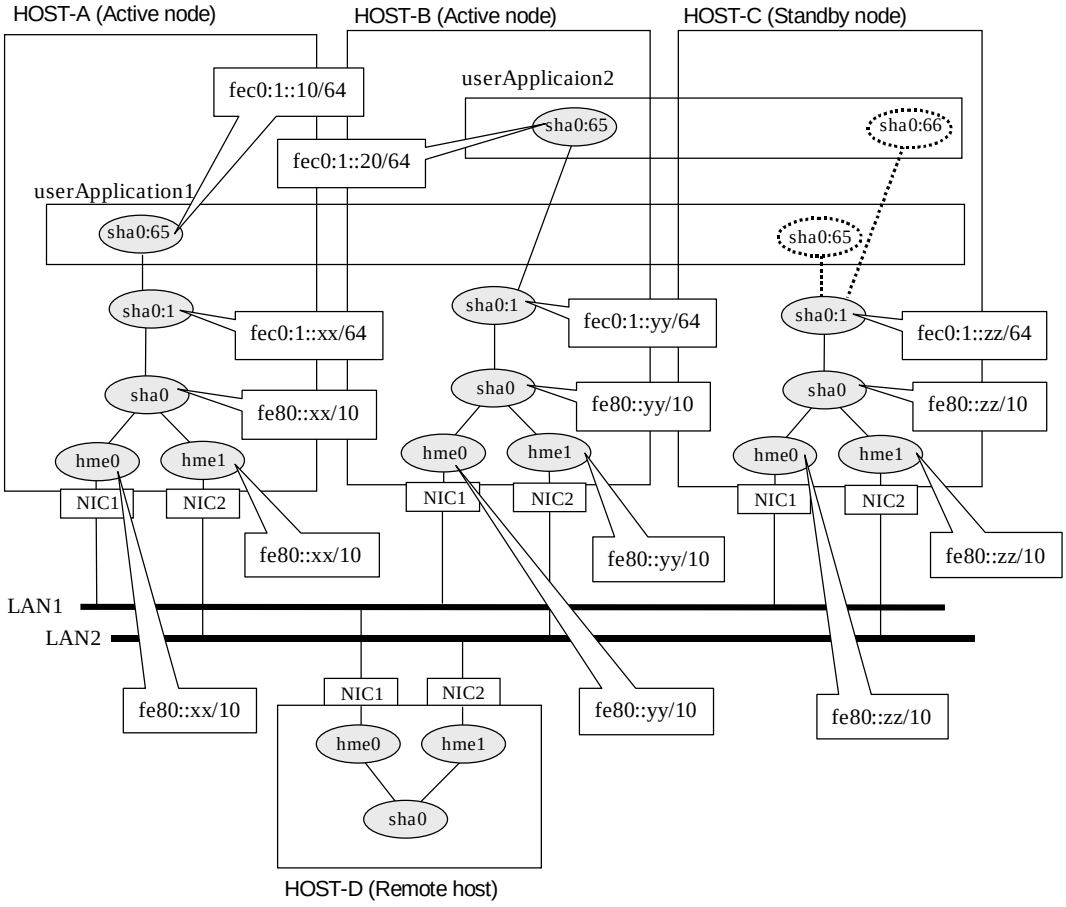
This section describes an example configuration procedure of the network shown in the diagram below.

The values for xx, yy and zz in the IP address of the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10        v6hosta1    # Takeover virtual IP (1)
fec0:1::20        v6hostb1    # Takeover virtual IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64

[HOST-C]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.
Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1
```

4) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of HOST-A, HOST-B, and HOST-C connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::10” and “fec0:1::20”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2.8 Example of the Cluster system (Cascade)

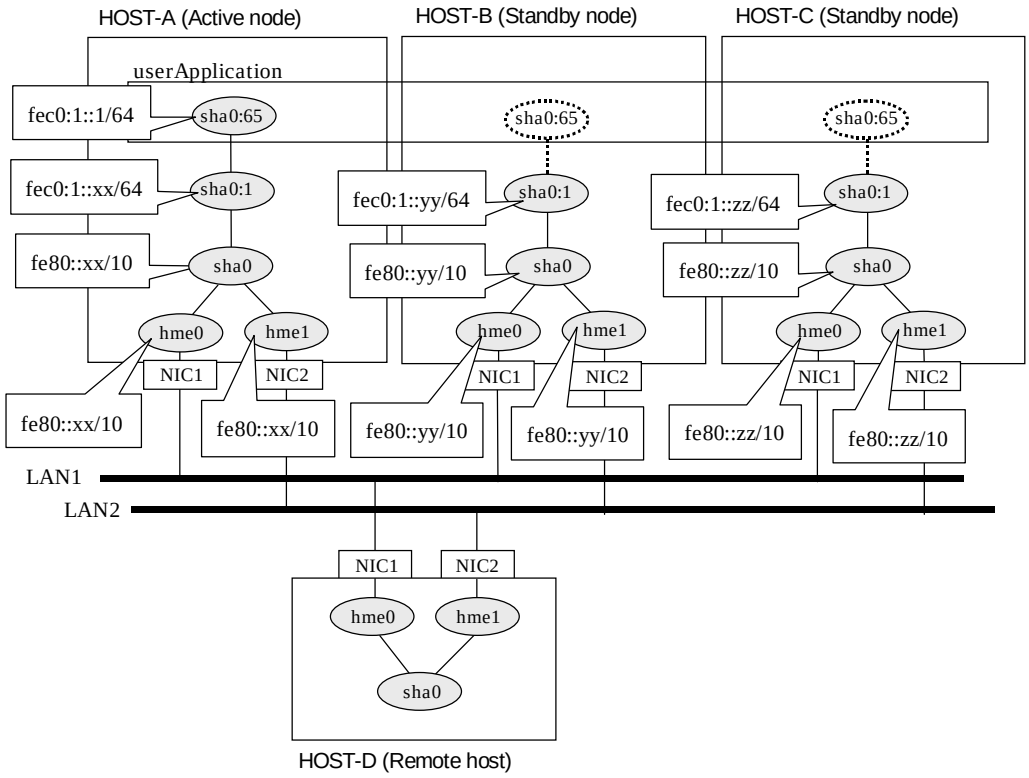
This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

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

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1          v6hosta1     # Takeover virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64

[HOST-C]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C.
Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::1”.

2) Starting of userApplication

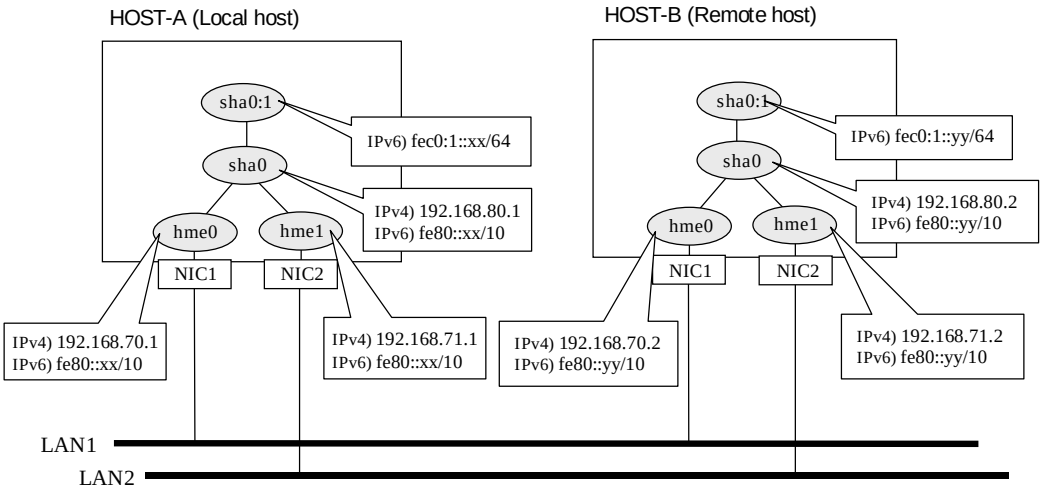
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3 Example of configuring Fast Switching mode (IPv4/IPv6)

B.3.1 Example of the Single system

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

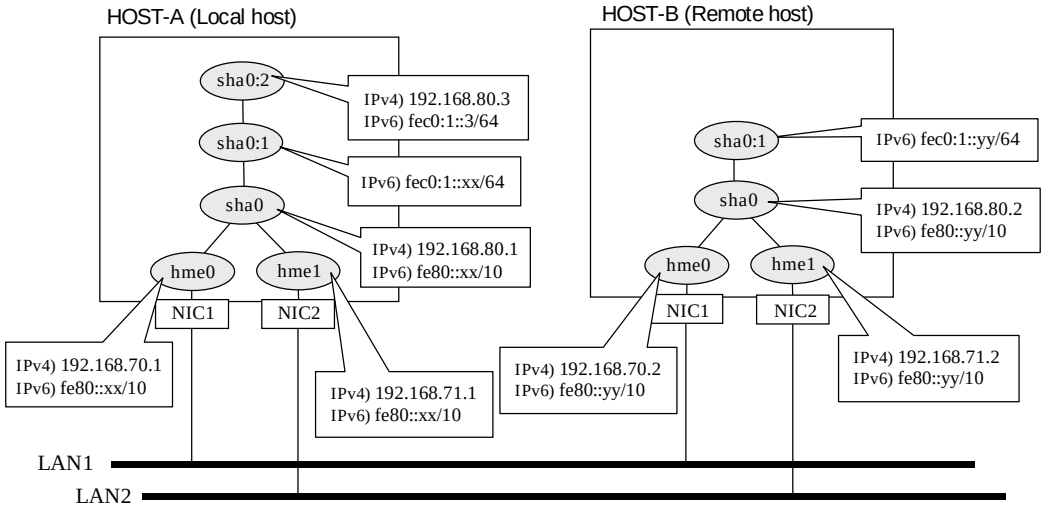
4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.3.2 Example of the Single system in Logical virtual interface

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.80.3    hosta1   # HOST-A Logical virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this,

it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::3          v6hosta1     # Logical virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of logical virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0:2 -i fec0:1::3/64

5) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

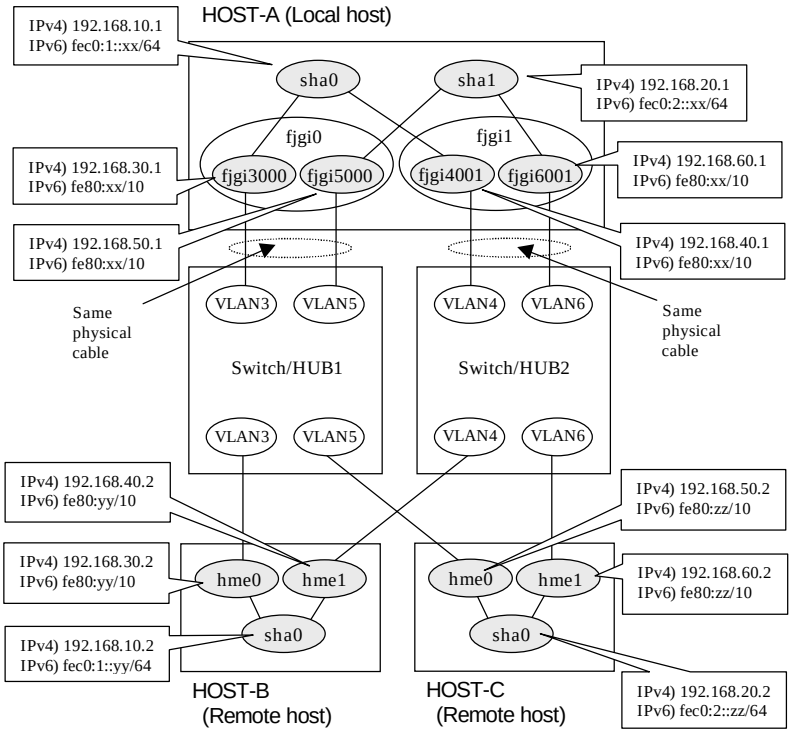
4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.3.3 Configuring virtual interfaces with tagged VLAN

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.10.1    hosta1    # HOST-A Virtual IP
192.168.20.1    hosta2    # HOST-A Virtual IP
192.168.30.1    hosta3    # HOST-A Physical IP (Tagged VLAN interface)
192.168.40.1    hosta4    # HOST-A Physical IP (Tagged VLAN interface)
192.168.50.1    hosta5    # HOST-B Physical IP (Tagged VLAN interface)
192.168.60.1    hosta6    # HOST-B Physical IP (Tagged VLAN interface)
192.168.10.2    hostb1    # HOST-B Virtual IP
192.168.30.2    hostb3    # HOST-B Physical IP
192.168.40.2    hostb4    # HOST-B Physical IP
192.168.20.2    hostc2    # HOST-C Virtual IP
192.168.50.2    hostc5    # HOST-C Physical IP
192.168.60.2    hostc6    # HOST-C Physical IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi3000

```
hosta3
```

- Contents of /etc/hostname.fjgi4001

```
hosta4
```

- Contents of /etc/hostname.fjgi5000

```
hosta5
```

- Contents of /etc/hostname.fjgi6001

```
hosta6
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.10.0      255.255.255.0
192.168.20.0      255.255.255.0
```

1-4) Create /etc/hostname6.fjgi3000, /etc/hostname6.fjgi4001, /etc/hostname6.fjgi5000 and /etc/hostname6.fjgi6001 files as an empty file.

1-5) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true   # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0               # sha0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 sha1               # sha1 sends Prefix "fec0:2::0/64".
```

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

2) Reboot

Run the following command to reboot the system. Make sure fjgi3000, fjgi4001, fjgi5000 and fjgi6001 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t fjgi3000,fjgi4001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t fjgi5000,fjgi6001

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -t fjgi3000,fjgi4001
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -t fjgi5000,fjgi6001

5) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hostb3
```

- Contents of /etc/hostname.hme1

```
hostb4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Create /etc/inet/ndpd.conf file and set the followings:

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

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hostc5
```

- Contents of /etc/hostname.hme1

```
hostc6
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true   # Every interface sends a router advertisement.
prefix fec0:2::0/64 sha0               # sha0 sends Prefix "fec0:2::0/64".
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

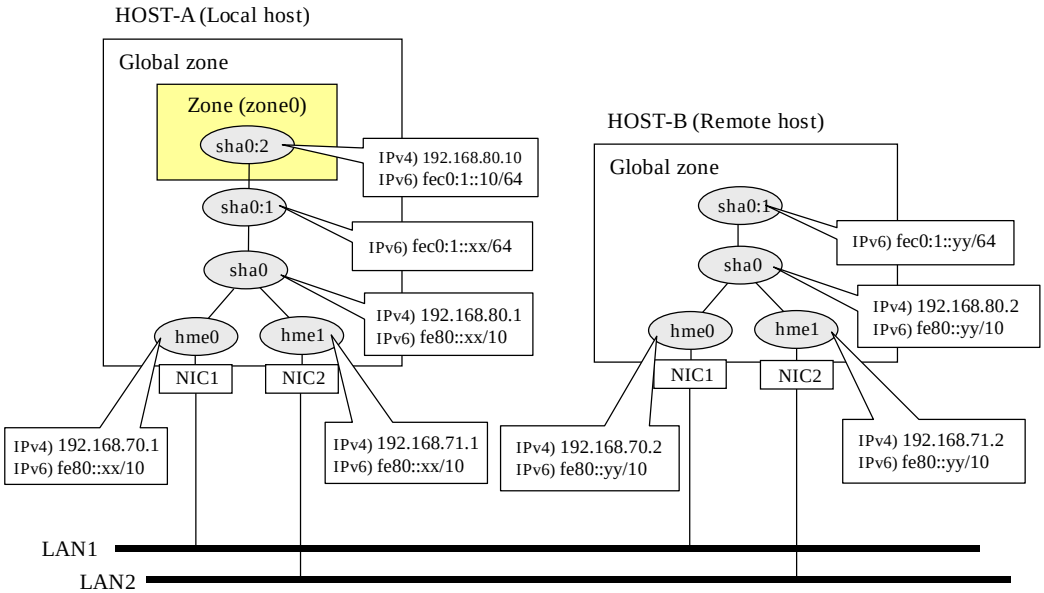
4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.3.4 Network configuration in the Solaris container

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1     host11    # HOST-A Physical IP (1)
192.168.71.1     host12    # HOST-A Physical IP (2)
192.168.80.1     hosta     # HOST-A Virtual IP
192.168.70.2     host21    # HOST-B Physical IP (1)
192.168.71.2     host22    # HOST-B Physical IP (2)
192.168.80.2     hostb     # HOST-B Virtual IP
192.168.80.10    zone0      # zone0 Logical IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0     255.255.255.0
192.168.71.0     255.255.255.0
192.168.80.0     255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

5) Set up a zone

Set up a zone by executing the following command:

/usr/sbin/zonecfg -z zone0

5-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

5-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in fast switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.80.10/24
zonecfg:zone0:net> set physical=sha0
zonecfg:zone0:net> end
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=sha0
zonecfg:zone0:net> end
```

The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.

5-3) Check the above setting.

```
zonecfg:zone0> export
```

5-4) Check setup consistency.

```
zonecfg:zone0> verify
```

5-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

6) Install the zone

Install the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 install

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

7) Start up the zone

Start up the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 boot

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.3.5 Example of the Cluster system (1:1 Standby)

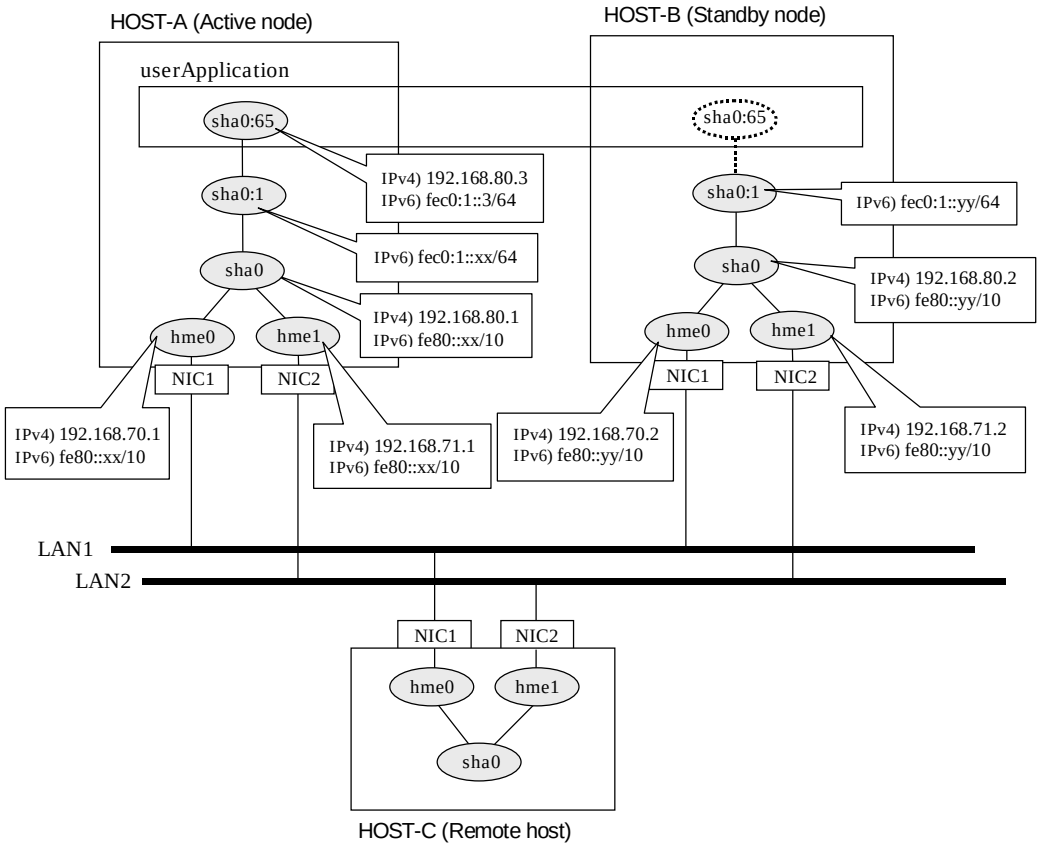
This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.80.3    hosta1   # Takeover virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
192.168.71.0      255.255.255.0
192.168.80.0      255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::3          v6hosta1     # Takeover virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3,fec0:1::3/64

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1
```

4) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3,fec0:1::3/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resource, select the SysNode for HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.3 - fec0:1::3”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3.6 Example of the Cluster system (Mutual standby)

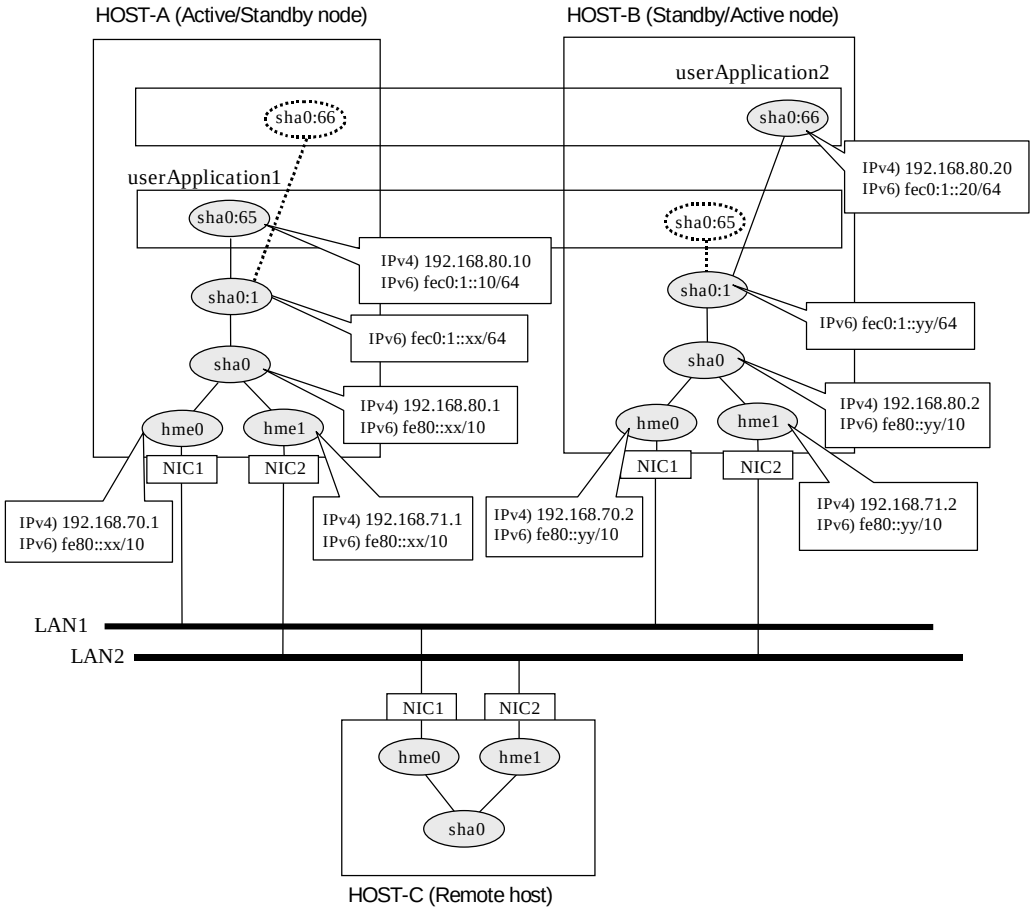
This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
```

```
192.168.80.10     hosta1   # Takeover virtual IP (1)
192.168.80.20     hostb1   # Takeover virtual IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
192.168.71.0      255.255.255.0
192.168.80.0      255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10        v6hosta1    # Takeover virtual IP (1)
fec0:1::20        v6hostb1    # Takeover virtual IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10,fec0:1::10/64
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20,fec0:1::20/64

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10,fec0:1::10/64
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20,fec0:1::20/64

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.10 - fec0:1::10” and “192.168.80.20 - fec0:1::20”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3.7 Example of the Cluster system (N:1 Standby)

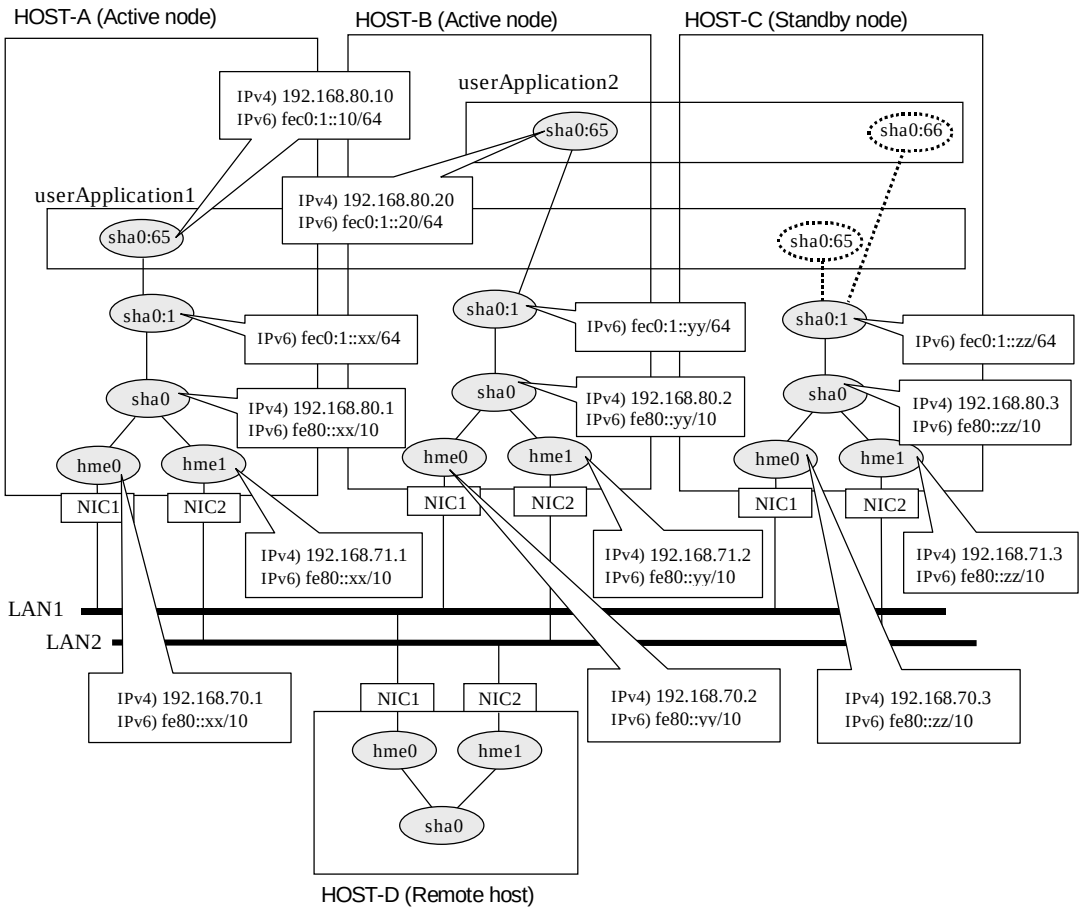
This section describes an example configuration procedure of the network shown in the diagram below.

The values for xx, yy and zz in the IP address of the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
```

```
192.168.71.2      host22   # HOST-B Physical IP (2)
192.168.80.2      hostb    # HOST-B Virtual IP
192.168.70.3      host31   # HOST-C Physical IP (1)
192.168.71.3      host32   # HOST-C Physical IP (2)
192.168.80.3      hostc    # HOST-C Virtual IP
192.168.80.10     hosta1   # Takeover virtual IP (1)
192.168.80.20     hostb1   # Takeover virtual IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
192.168.71.0      255.255.255.0
192.168.80.0      255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10        v6hosta1    # Takeover virtual IP (1)
fec0:1::20        v6hostb1    # Takeover virtual IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10,fec0:1::10/64

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1
```

4) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20,fec0:1::20/64
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host31
```

- Contents of /etc/hostname.hme1

```
host32
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1
```

4) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10,fec0:1::10/64
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20,fec0:1::20/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of HOST-A, HOST-B, and HOST-C connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C.
Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.10 - fec0:1::10” and “192.168.80.20 - fec0:1::20”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3.8 Example of the Cluster system (Cascade)

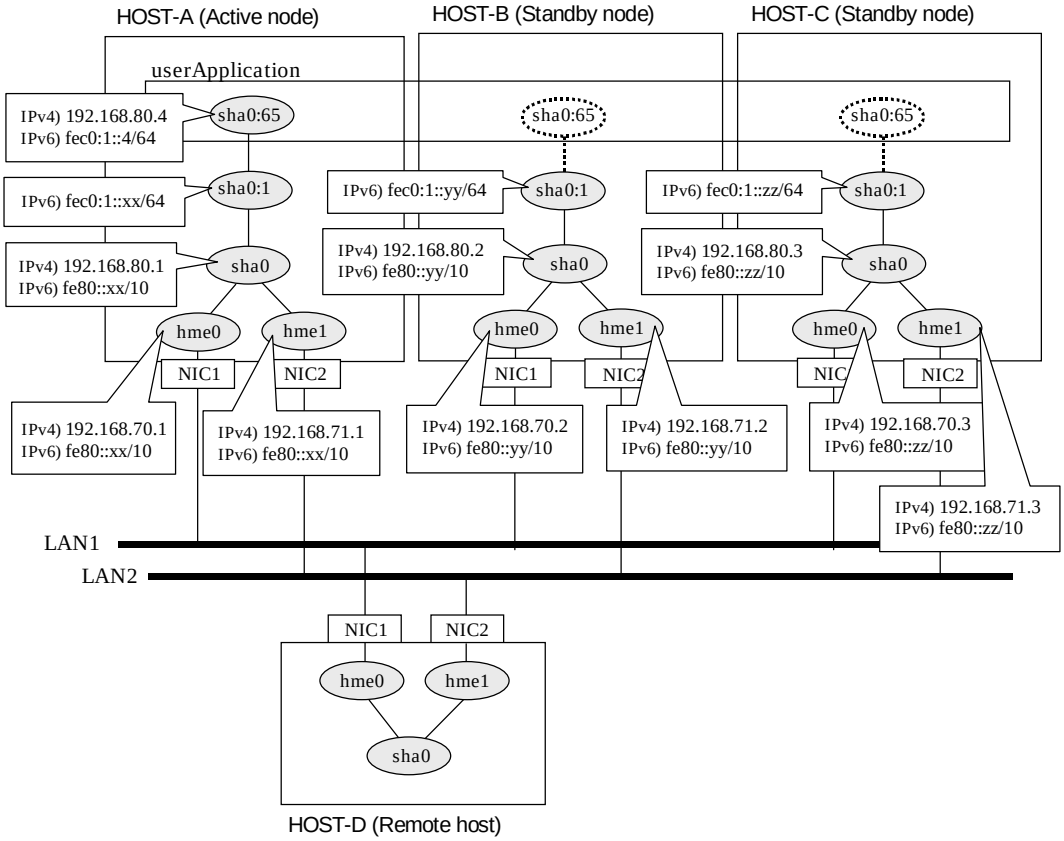
This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP (1)
192.168.71.1    host12   # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21   # HOST-B Physical IP (1)
192.168.71.2    host22   # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.70.3    host31   # HOST-C Physical IP (1)
```

```
192.168.71.3      host32   # HOST-C Physical IP (2)
192.168.80.3      hostc    # HOST-C Virtual IP
192.168.80.4      hosta1   # Takeover virtual IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
192.168.71.0      255.255.255.0
192.168.80.0      255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

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

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::4          v6hosta1    # Takeover virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4,fec0:1::4/64

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4,fec0:1::4/64

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host31
```

- Contents of /etc/hostname.hme1

```
host32
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme1 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t hme0,hme1

4) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4,fec0:1::4/64

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C.
Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the

takeover address “192.168.80.4 - fec0:1::4”.

2) Starting of userApplication

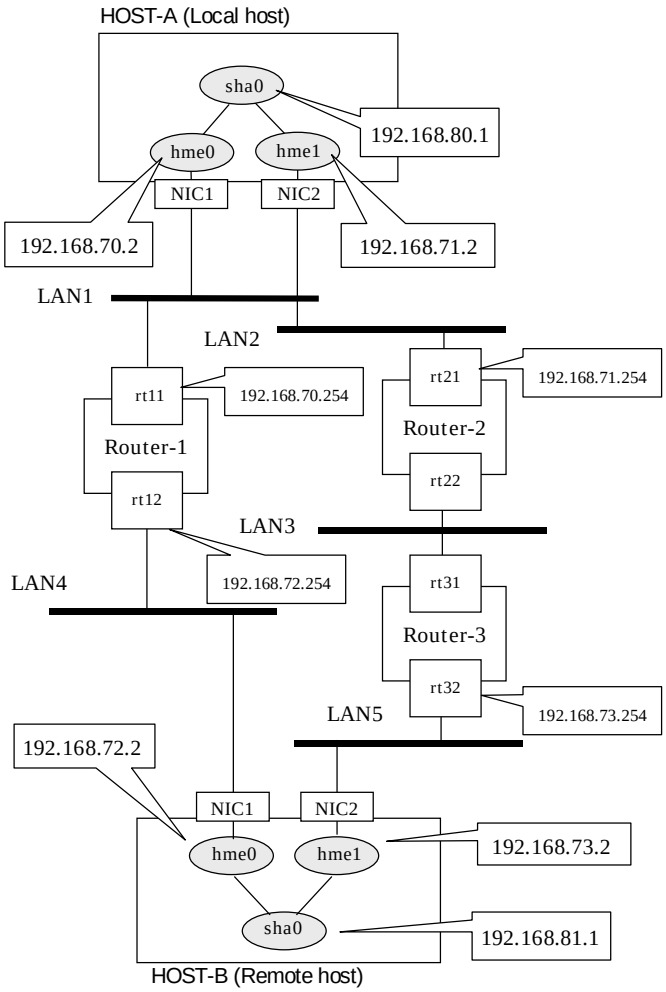
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.4 Example of configuring RIP mode

B.4.1 Example of the Single system

This section describes an example configuration procedure of the network shown in the diagram below.

If the router monitoring function is not used, omit 4) and 6) in the procedure for setting up on each host.



Note) rt11,rt12,rt21,rt22,rt31 and rt32 mean the host name of each router.

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.2     host11   # HOST-A Physical IP (1)
192.168.71.2     host12   # HOST-A Physical IP (2)
192.168.80.1     hosta    # HOST-A Virtual IP
192.168.72.2     host21   # HOST-B Physical IP (1)
192.168.73.2     host22   # HOST-B Physical IP (2)
192.168.81.1     hostb    # HOST-B Virtual IP
192.168.70.254   rt11     # ROUTER-1 Physical IP (1)
192.168.71.254   rt21     # ROUTER-2 Physical IP (1)
```

```
192.168.72.254   rt12     # ROUTER-1 Physical IP (2)
192.168.73.254   rt32     # ROUTER-3 Physical IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0     255.255.255.0
192.168.71.0     255.255.255.0
192.168.72.0     255.255.255.0
192.168.73.0     255.255.255.0
192.168.80.0     255.255.255.0
192.168.81.0     255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i 192.168.80.1 -t hme0,hme1

4) Setting up the router monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.254,192.168.71.254

5) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

6) Starting the router monitoring function

The following is an example where monitoring is performed 5 times at the interval of 4 seconds, and if monitoring fails 6 consecutive times, the router monitoring function is stopped:

/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5 -r 6

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme1

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i 192.168.81.1 -t hme0,hme1

4) Setting up the router monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.72.254,192.168.73.254

5) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

6) Starting the router monitoring function

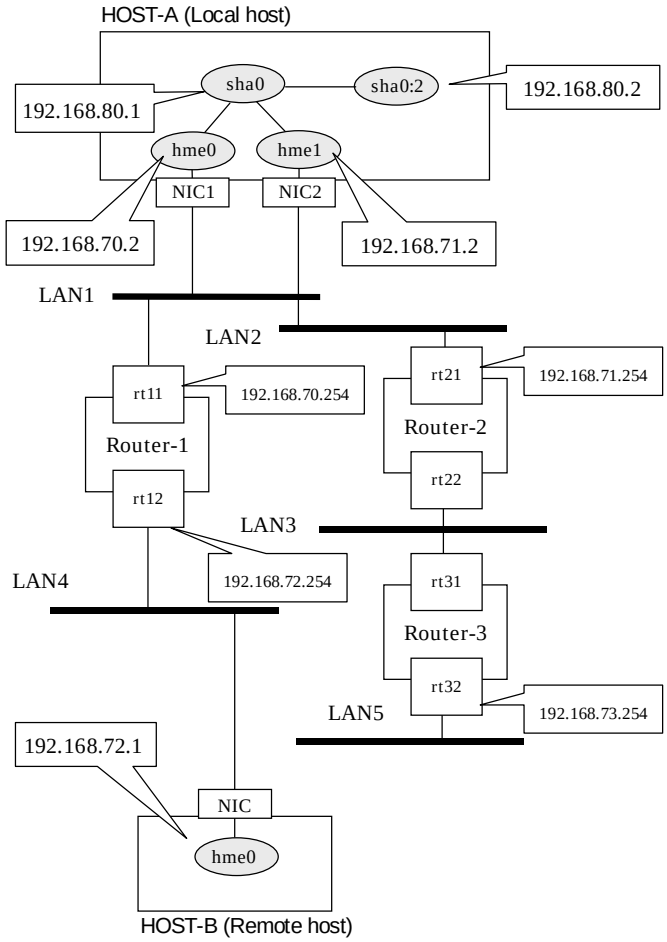
The following is an example where monitoring is performed 5 times at the interval of 4 seconds, and if monitoring fails 6 consecutive times, the router monitoring function is stopped:

/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5 -r 6

B.4.2 Example of the Single system in Logical virtual interface

This section describes an example configuration procedure of the network shown in the diagram below.

If the router monitoring function is not used, omit 5) and 7) in the procedure for setting up on HOST-A.



Note) rt11,rt12,rt21,rt22,rt31 and rt32 mean the host name of each router.

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.2     host11   # HOST-A Physical IP (1)
192.168.71.2     host12   # HOST-A Physical IP (2)
192.168.80.1     hosta    # HOST-A Virtual IP
192.168.80.2     hosta2   # HOST-A Logical virtual IP
192.168.72.2     host21   # HOST-B Physical IP (1)
192.168.73.2     host22   # HOST-B Physical IP (2)
192.168.81.1     hostb    # HOST-B Virtual IP
192.168.70.254   rt11     # ROUTER-1 Physical IP (1)
192.168.71.254   rt21     # ROUTER-2 Physical IP (1)
192.168.72.254   rt12     # ROUTER-1 Physical IP (2)
192.168.73.254   rt32     # ROUTER-3 Physical IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme1

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.72.0    255.255.255.0
192.168.73.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i 192.168.80.1 -t hme0,hme1

4) Creation of logical virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.2

5) Setting up the router monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create –n sha0 -p 192.168.70.254,192.168.71.254

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the router monitoring function

The following is an example where monitoring is performed 5 times at the interval of 4 seconds, and if monitoring fails 6 consecutive times, the router monitoring function is stopped:

/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5 -r 6

[HOST-B]

1) Setting up the remote system

A system possible to use is optional, and its setting of the system network environment is executed.

B.5 Example of configuring Fast switching/RIP mode

B.5.1 Example of the Single system

For the configuration example of Fast switching/RIP mode, refer to “B.1.1 Example of the Single system” and “B.4.1 Example of the Single system”.

B.5.2 Example of the Single system in Logical virtual interface

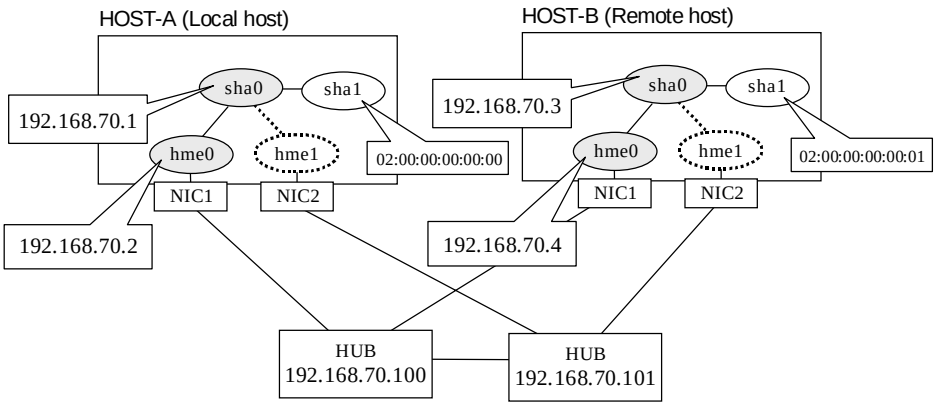
For the configuration example of Fast swiching/RIP mode using a logical virtual interface, refer to “B.1.2 Example of the Single system in Logical virtual interface” and “B.4.2 Example of the Single system in Logical virtual interface”.

B.6 Example of configuring NIC switching mode (IPv4)

B.6.1 Example of the Single system without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A Virtual IP
192.168.70.2      host11    # HOST-A Physical IP
192.168.70.3      hostb     # HOST-B Virtual IP
192.168.70.4      host21    # HOST-B Physical IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

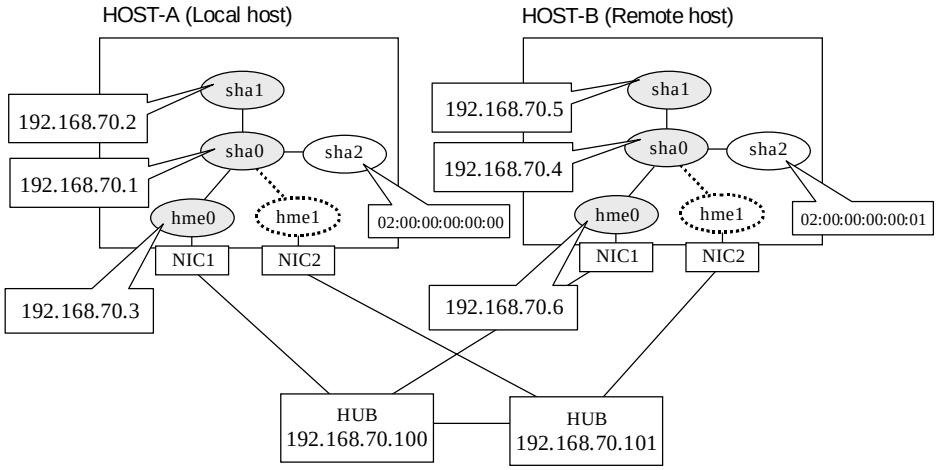
7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

B.6.2 Example of the Single system with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta1   # HOST-A Virtual IP (1)
192.168.70.2      hosta2   # HOST-A Virtual IP (2)
192.168.70.3      host11   # HOST-A Physical IP
192.168.70.4      hostb1   # HOST-B Virtual IP (1)
192.168.70.5      hostb1   # HOST-B Virtual IP (2)
192.168.70.6      host21   # HOST-B Physical IP
192.168.70.100    swhub1   # Primary HUB IP
192.168.70.101    swhub2   # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1
/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/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t hme0,hme1
/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/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

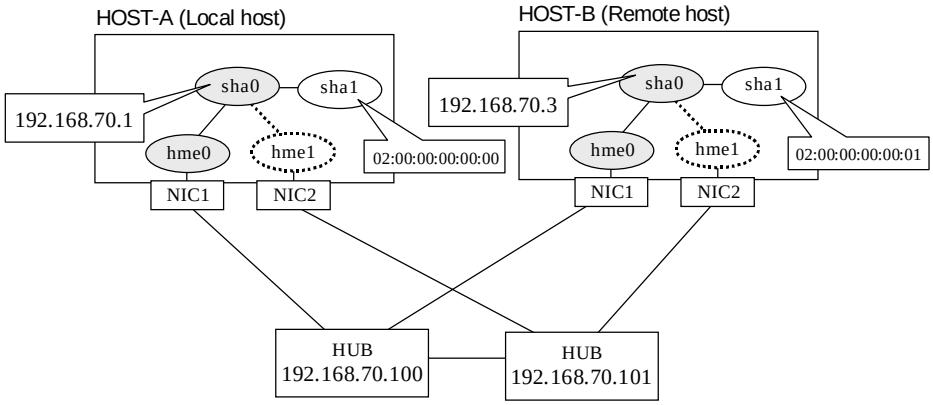
7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

B.6.3 Example of the Single system in Physical IP address takeover function

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A Virtual IP
192.168.70.3      hostb     # HOST-B Virtual IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hosta
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hostb
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Activation of virtual interface

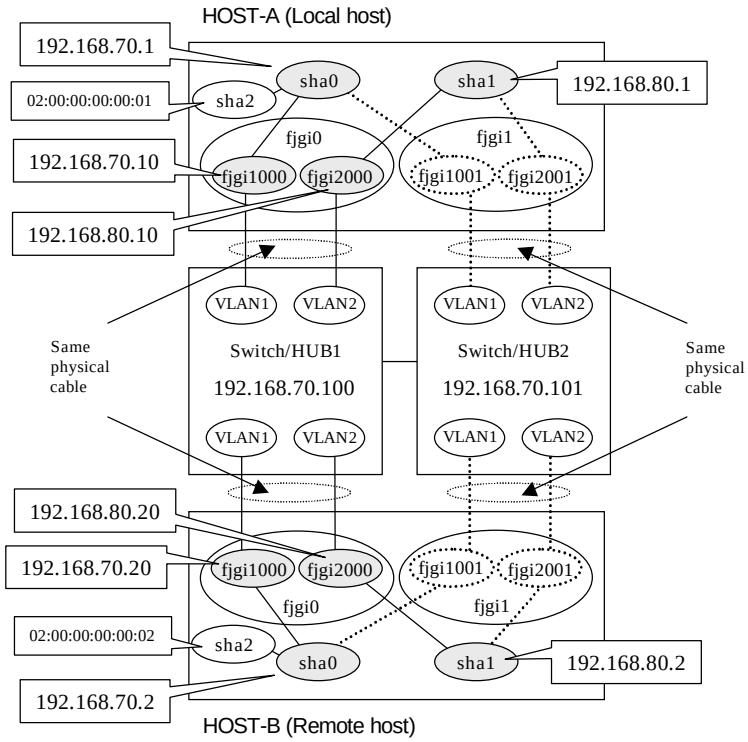
/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

B.6.4 Configuring virtual interfaces with tagged VLAN (synchronized 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/inet/hosts file.

```
192.168.70.1     hosta     # HOST-A Virtual IP
192.168.70.10    host71    # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1     hostb     # HOST-A Virtual IP
192.168.80.10    host81    # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2     hostc     # HOST-B Virtual IP
192.168.70.20    host72    # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2     hostd     # HOST-B Virtual IP
192.168.80.20    host82    # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100   swhub1    # Primary Switchi/HUB IP
192.168.70.101   swhub2    # Secondary Switch/HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host71
```

- Contents of /etc/hostname.fjgi2000

```
host81
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t fjgi2000,fjgi2001

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.fjgi2000.

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on

4) Setting up the HUB monitoring function (Synchronized switching)

/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0

6) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2000 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host72
```

- Contents of /etc/hostname.fjgi2000

```
host82
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t fjgi2000,fjgi2001

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.fjgi2000.

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on

4) Setting up the HUB monitoring function (Synchronized switching)

/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0

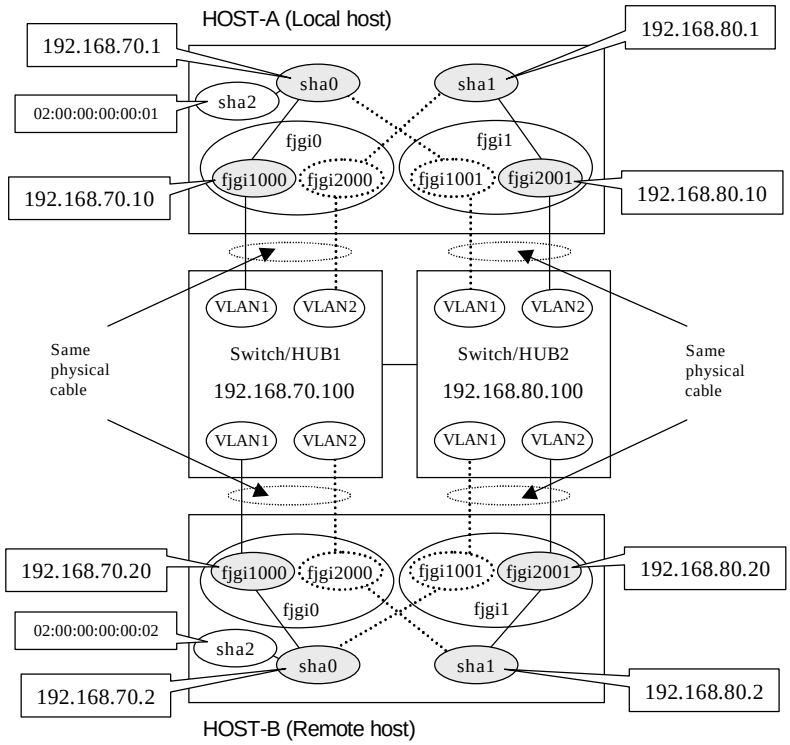
6) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2000 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

B.6.5 Configuring virtual interfaces with tagged VLAN (asynchronized 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/inet/hosts file.

```
192.168.70.1     hosta     # HOST-A Virtual IP
192.168.70.10    host71    # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1     hostb     # HOST-A Virtual IP
192.168.80.10    host81    # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2     hostc     # HOST-B Virtual IP
192.168.70.20    host72    # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2     hostd     # HOST-B Virtual IP
192.168.80.20    host82    # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100   swhub1    # Switch/HUB1 IP
192.168.80.100   swhub2    # Switch/HUB2 IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host71
```

- Contents of /etc/hostname.fjgi2001

```
host81
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t fjgi2001,fjgi2000

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.fjgi2001.

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0

5) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2001 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host72
```

- Contents of /etc/hostname.fjgi2001

```
host82
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t fjgi2001,fjgi2000

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.fjgi2001.

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off
```

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0
```

5) Reboot

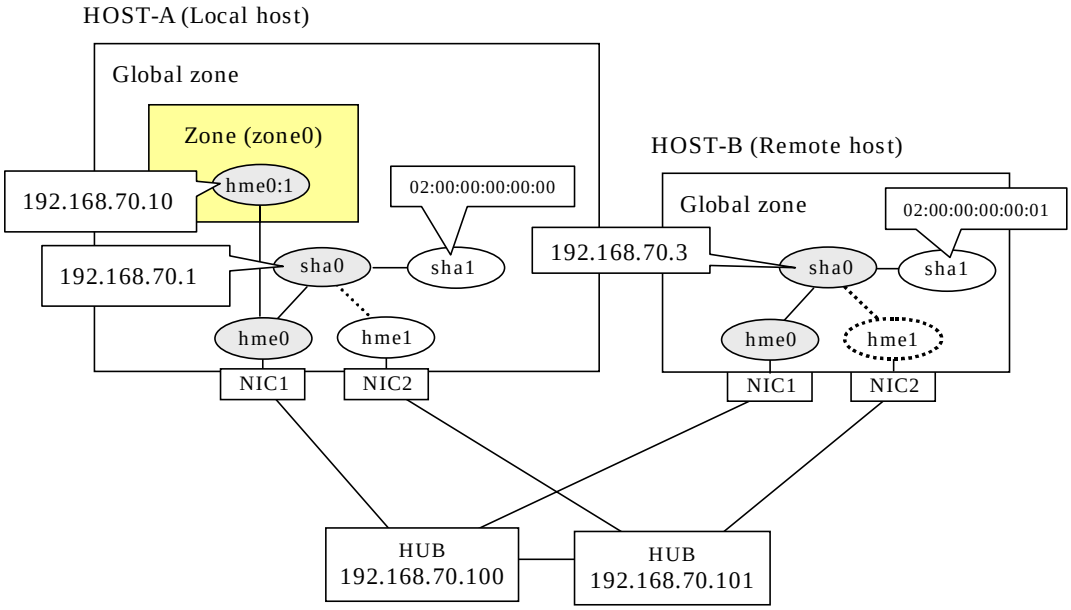
Run the following command to reboot the system. Make sure fjgi1000 and fjgi2001 are enabled as IPv4 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

B.6.6 Network configuration in the Solaris container (physical IP takeover)

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta      # HOST-A Virtual IP
192.168.70.3      hostb      # HOST-B Virtual IP
192.168.70.10     zone0       # zone0 Logical IP
192.168.70.100    swhub1      # Primary HUB IP
192.168.70.101    swhub2      # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hosta
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t hme0,hme1

Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Change the method of deactivating the standby interface

/opt/FJSVhanet/usr/sbin/hanetparam -d plumb

7) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Set up a zone

Set up a zone by executing the following command:

/usr/sbin/zonecfg -z zone0

9-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

9-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in NIC switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.70.10/24
zonecfg:zone0:net> set physical=hme0
zonecfg:zone0:net> end
```

If you specify the redundant physical interface in NIC switching mode, specify the primary physical interface.

9-3) Check the above setting.

```
zonecfg:zone0> export
```

9-4) Check setup consistency.

```
zonecfg:zone0> verify
```

9-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

10) Install the zone

Install the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 install

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

11) Start up the zone

Start up the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 boot

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
hostb
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t hme0,hme1

Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

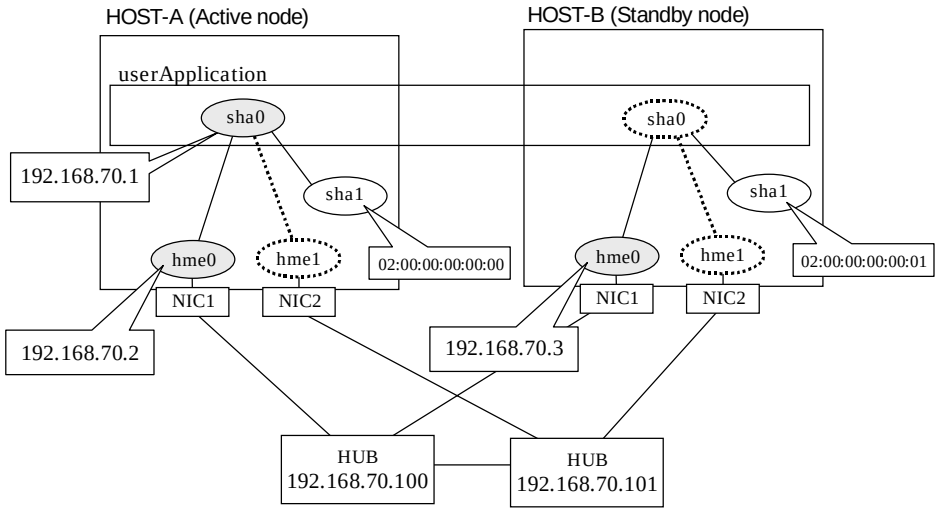
/opt/FJSVhanet/usr/sbin/hanetpoll on

B.6.7 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B Virtual IP (Takeover IP)
192.168.70.2      host11    # HOST-A Physical IP
192.168.70.3      host21    # HOST-B Physical IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resource, select the SysNode for HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1”.

2) Starting of userApplication

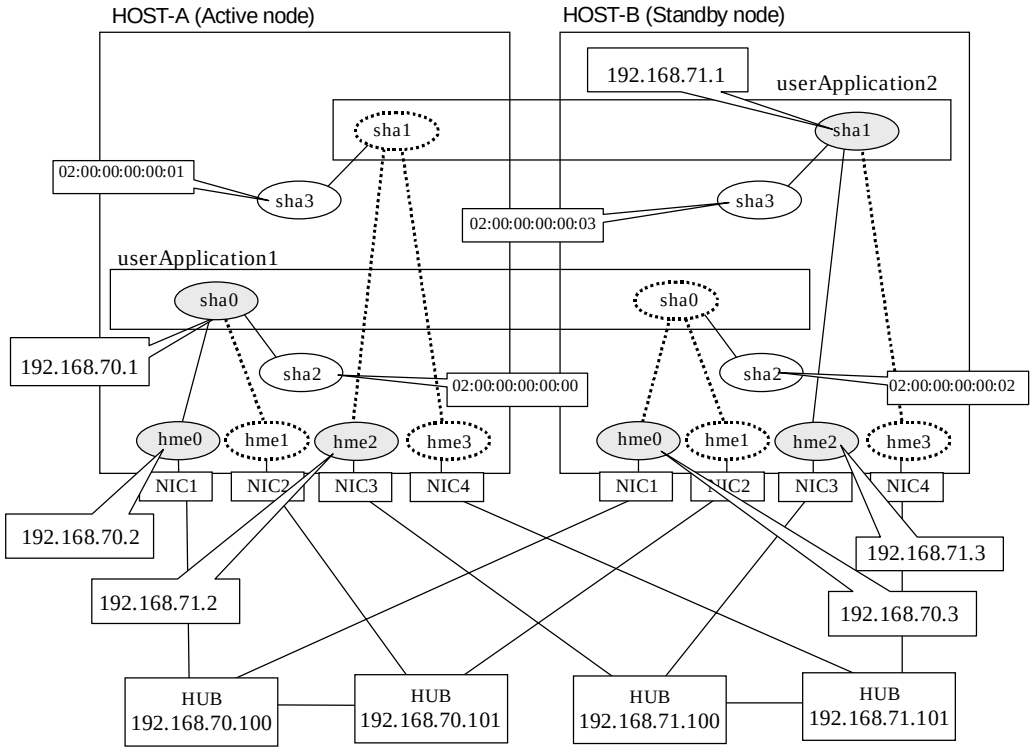
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.8 Example of the Cluster system (Mutual standby) without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2      host11    # HOST-A Physical IP (1)
192.168.70.3      host21    # HOST-B Physical IP (1)
192.168.71.1      hostb     # HOST-A/B Virtual IP (Takeover IP2)
192.168.71.2      host12    # HOST-A Physical IP (2)
192.168.71.3      host22    # HOST-B Physical IP (2)
192.168.70.100    swhub1    # Primary HUB IP (1)
192.168.70.101    swhub2    # Secondary HUB IP (1)
192.168.71.100    swhub3    # Primary HUB IP (2)
192.168.71.101    swhub4    # Secondary HUB IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme2

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme2 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t hme2,hme3

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0 and /etc/hostname.hme2.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.71.100,192.168.71.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -a 02:00:00:00:00:01 -t sha1

6) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha2
/opt/FJSVhanet/usr/sbin/strptl -n sha3

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme2

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme2 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t hme2,hme3

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0 and /etc/hostname.hme2.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.71.100,192.168.71.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -a 02:00:00:00:00:03 -t sha1

6) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha2
/opt/FJSVhanet/usr/sbin/strptl -n sha3

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1” and “192.168.71.1”.

2) Starting of userApplication

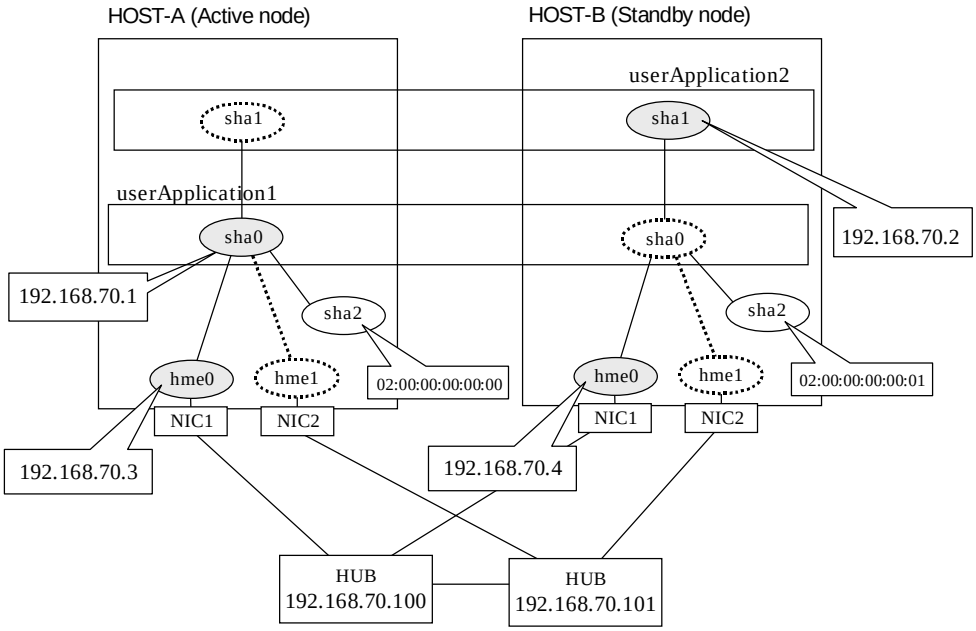
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.9 Example of the Cluster system (Mutual standby) with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2      hostb     # HOST-A/B Virtual IP (Takeover IP2)
192.168.70.3      host11    # HOST-A Physical IP
192.168.70.4      host21    # HOST-B Physical IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1
/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/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0

6) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha2

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t hme0,hme1
/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/hostname.hme0.

4) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0
```

6) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

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

8) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1” and “192.168.70.2”.

2) Starting of userApplication

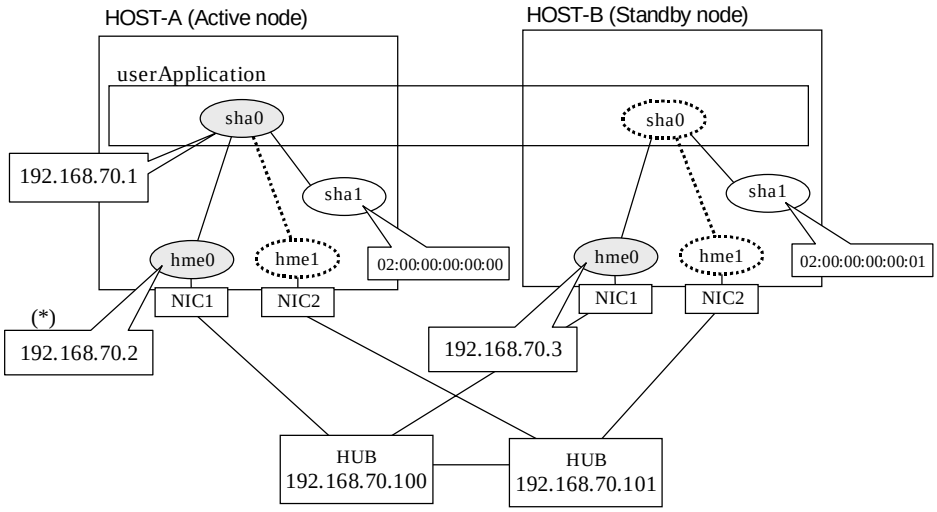
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.10 Example of the Cluster system in Physical IP address takeover function I

This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for enabling physical interface on a standby node.)

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



*) Physical IP address (192.168.70.2) is inactivated when takeover IP address (192.168.70.1) is activated.

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta    # HOST-A/B Virtual IP (Takeover IP)
192.168.70.2      host11   # HOST-A Physical IP
192.168.70.3      host21   # HOST-B Physical IP
192.168.70.100    swhub1   # Primary HUB IP
192.168.70.101    swhub2   # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1”.

2) Starting of userApplication

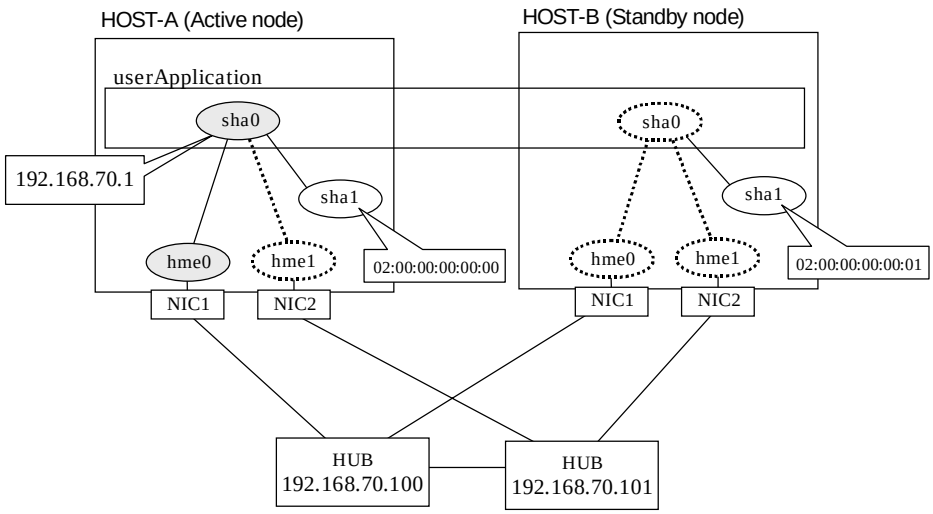
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.11 Example of the Cluster system in Physical IP address takeover function II

This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for not enabling physical interface on a standby node.)

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 4) and 7) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B Virtual IP (Takeover IP)
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t hme0,hme1

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

4) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

5) Creation of takeover virtual interface

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

6) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

7) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t hme0,hme1

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

4) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

5) Creation of takeover virtual interface

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

6) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

7) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 7) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1”.

2) Starting of userApplication

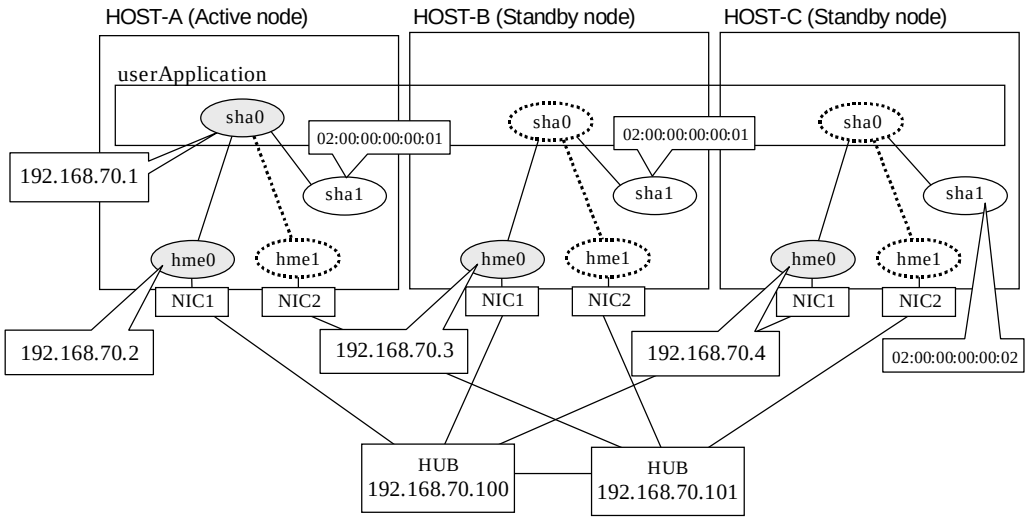
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.12 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B/C Virtual IP (Takeover IP)
192.168.70.2      host11    # HOST-A Physical IP
192.168.70.3      host21    # HOST-B Physical IP
192.168.70.4      host31    # HOST-C Physical IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
Host31
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:02 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C.
Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the

takeover address “192.168.70.1”.

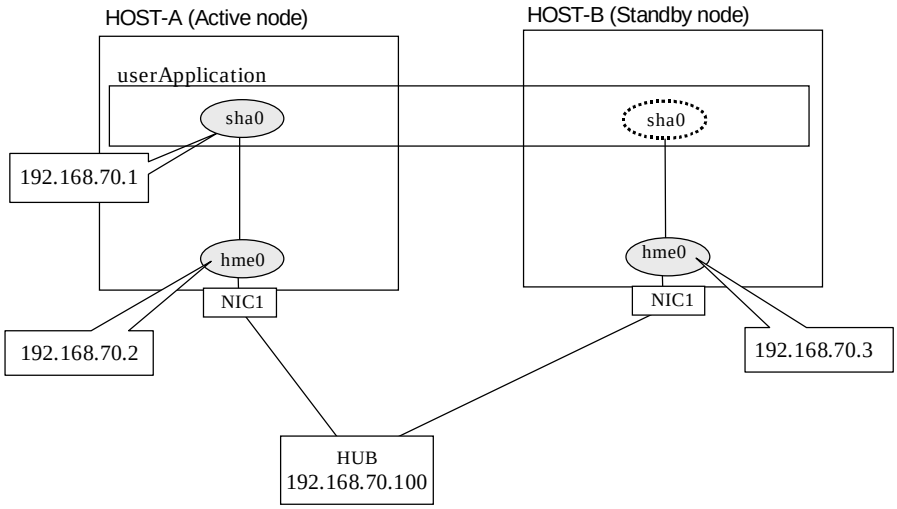
2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.13 Example of the Cluster system (NIC non-redundant)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B Virtual IP (Takeover IP)
192.168.70.2      host11    # HOST-A Physical IP
192.168.70.3      host21    # HOST-B Physical IP
192.168.70.100    swhub1    # Primary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0

Ensure that the physical IP address specified using option '-e' is the same IP address configured

in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off

5) Creation of takeover virtual interface

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

6) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off

5) Creation of takeover virtual interface

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

6) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 6) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.
To create Gls resource, select the SysNode for HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.7 Example of configuring NIC switching mode (IPv6)

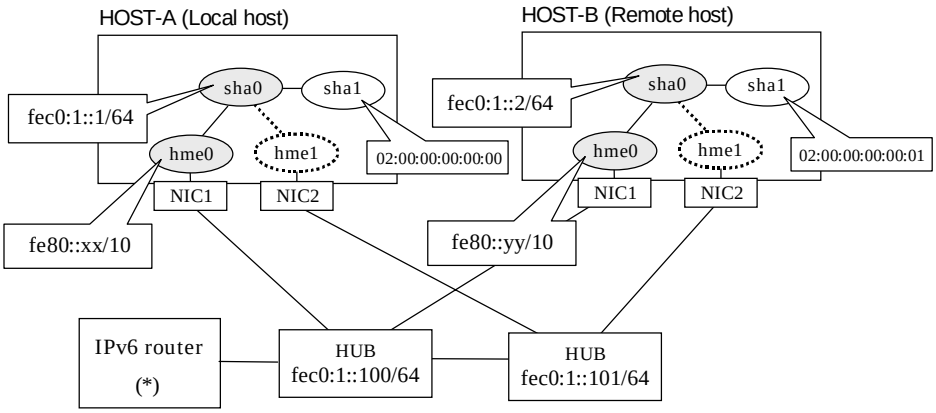
When using IPv6 address, it is required to set an IPv6 router on the same network. Also, specify the same prefix and prefix length of IPv6 address for redundant control line function configured in the IPv6 router.

B.7.1 Example of the Single system without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta          # HOST-A Virtual IP
fec0:1::2       v6hostb          # HOST-B Virtual IP
fec0:1::100     swhub1            # Primary HUB IP
fec0:1::101     swhub2            # Secondary HUB IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

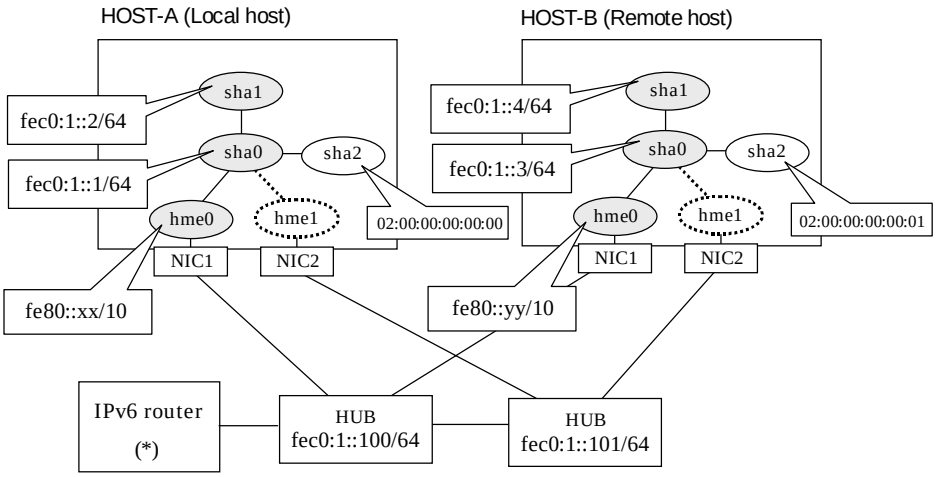
/opt/FJSVhanet/usr/sbin/hanetpoll on

B.7.2 Example of the Single system with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta1        # HOST-A Virtual IP (1)
fec0:1::2       v6hosta2        # HOST-A Virtual IP (2)
fec0:1::3       v6hostb1        # HOST-B Virtual IP (1)
fec0:1::4       v6hostb2        # HOST-B Virtual IP (2)
fec0:1::100     swhub1           # Primary HUB IP
fec0:1::101     swhub2           # Secondary HUB IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

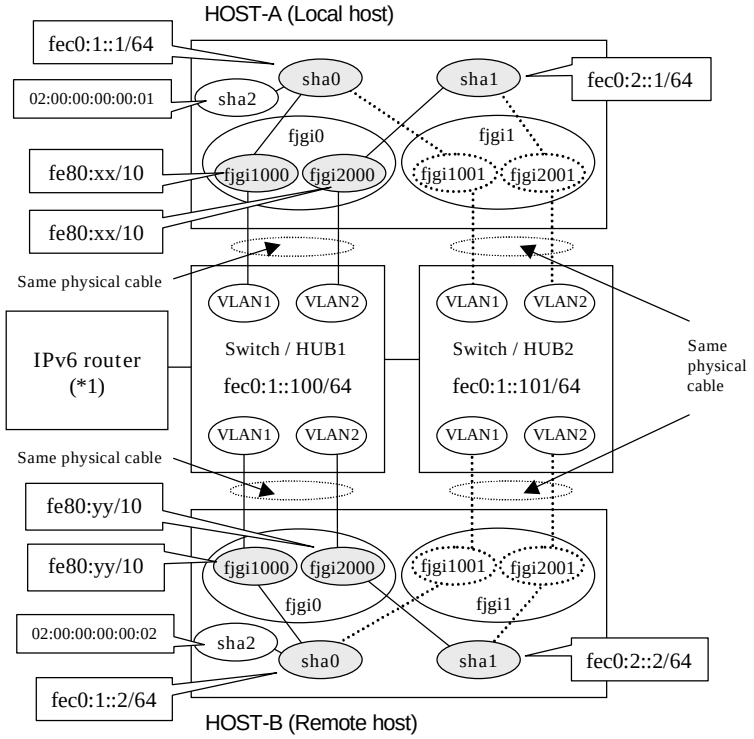
/opt/FJSVhanet/usr/sbin/hanetpoll on

B.7.3 Configuring virtual interfaces with tagged VLAN (synchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

```
ifdefault AdvSendAdvertisements true    # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi1000            # fjgi1000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi2000            # fjgi2000 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2000 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta1    # HOST-A Virtual IP(1)
fec0:2::1       v6hosta2    # HOST-A Virtual IP(2)
fec0:1::2       v6hostb1    # HOST-B Virtual IP(1)
fec0:2::2       v6hostb2    # HOST-B Virtual IP(2)
```

```
fec0:1::100     swhub1     # primary HUB IP
fec0:1::101     swhub2     # secondary HUB IP
```

2) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t fjgi2000,fjgi2001
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b on
```

4) Setting up the HUB monitoring function (Synchronized switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0
```

6) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2000 are enabled as IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2000 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t fjgi2000,fjgi2001
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b on
```

4) Setting up the HUB monitoring function (Synchronized switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0
```

6) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2000 are enabled as IPv6 interfaces after rebooting the system.

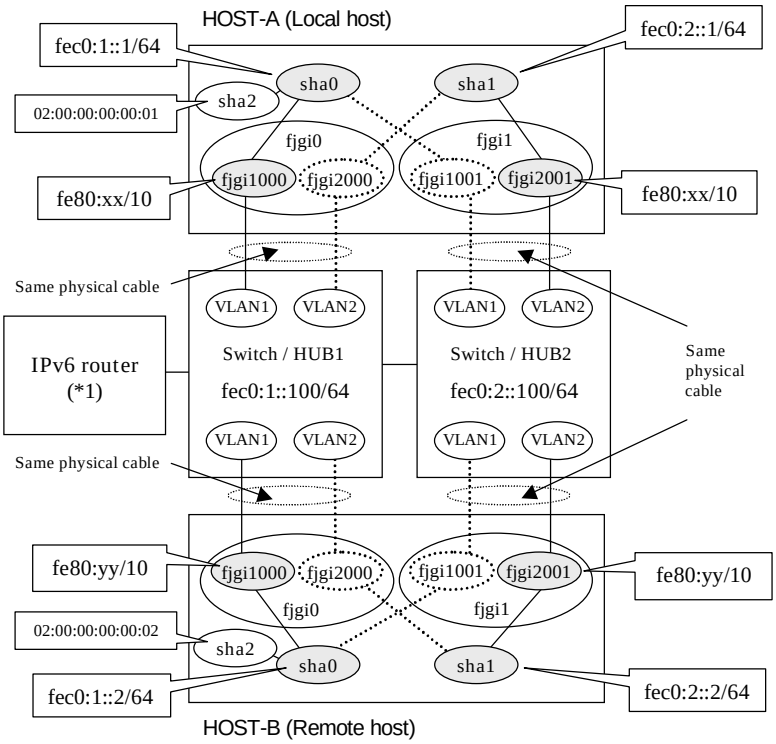
```
/usr/sbin/shutdown -y -i6 -g0
```

B.7.4 Configuring virtual interfaces with tagged VLAN (asynchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 4) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

```
ifdefault AdvSendAdvertisements true    # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi1000                # fjgi1000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi2001                # fjgi2001 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2001 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1          v6hosta1     # HOST-A Virtual IP(1)
fec0:2::1          v6hosta2     # HOST-A Virtual IP(2)
fec0:1::2          v6hostb1     # HOST-B Virtual IP(1)
fec0:2::2          v6hostB2     # HOST-B Virtual IP(2)
```

```
fec0:1::100     swhub1     # Switch/HUB1 IP
fec0:2::100     swhub2     # Switch/HUB2 IP
```

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t fjgi2001,fjgi2000

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100 -b off

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0

5) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2001 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2001 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t fjgi2001,fjgi2000

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100 -b off

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0

5) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2001 are enabled as IPv6 interfaces after rebooting the system.

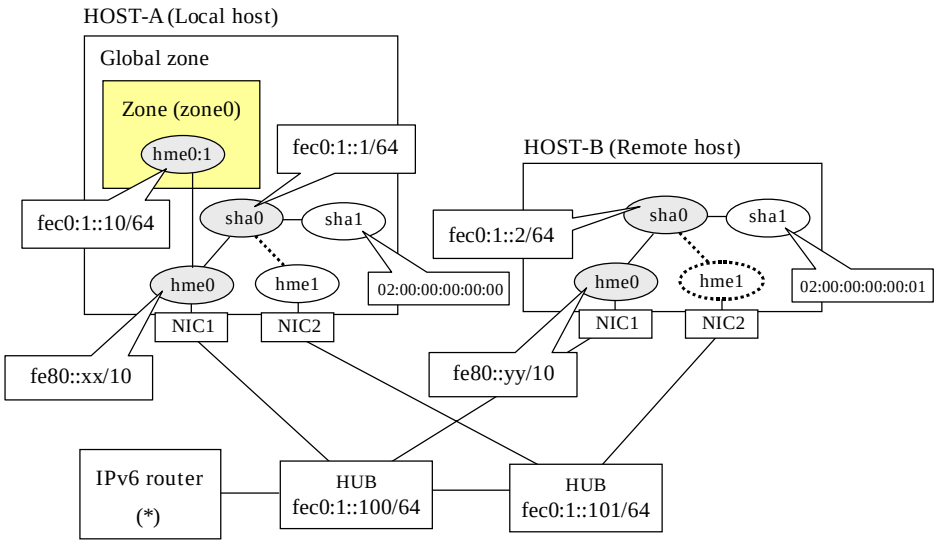
/usr/sbin/shutdown -y -i6 -g0

B.7.5 Network configuration in the Solaris container (logical IP takeover)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta     # HOST-A Virtual IP
fec0:1::2       v6hostb     # HOST-B Virtual IP
fec0:1::100     swhub1       # Primary HUB IP
fec0:1::101     swhub2       # Secondary HUB IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Change the method of deactivating the standby interface

/opt/FJSVhanet/usr/sbin/hanetparam -d plumb

7) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Set up a zone

Set up a zone by executing the following command:

/usr/sbin/zonecfg -z zone0

9-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

9-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in NIC switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=hme0
zonecfg:zone0:net> end
```

The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.
If you specify the redundant physical interface in NIC switching mode, specify the primary physical interface.

9-3) Check the above setting.

```
zonecfg:zone0> export
```

9-4) Check setup consistency.

```
zonecfg:zone0> verify
```

9-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

10) Install the zone

Install the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 install

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

11) Start up the zone

Start up the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 boot

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

B.7.6 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

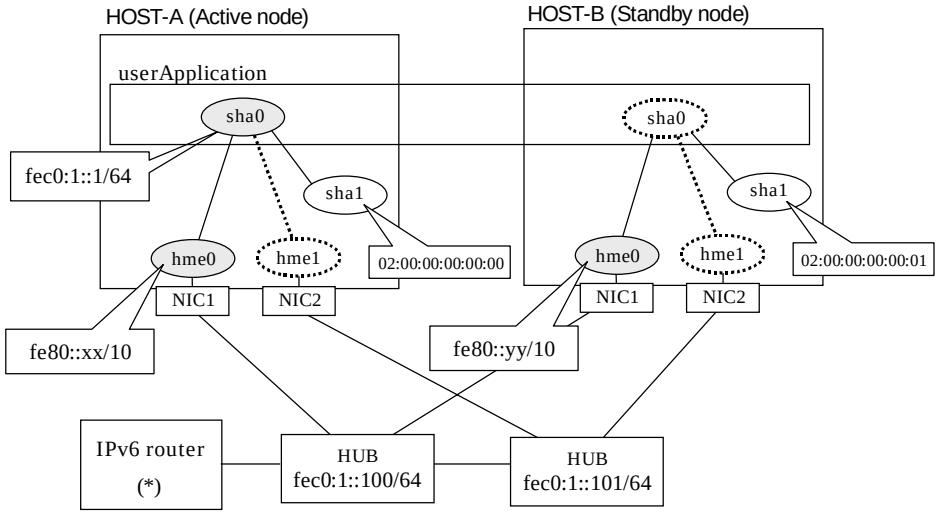
The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta        # HOST-A/B Takeover virtual IP
fec0:1::100     swhub1           # Primary HUB IP
fec0:1::101     swhub2           # Secondary HUB IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resource, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::1”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.7.7 Example of the Cluster system (Mutual standby) without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

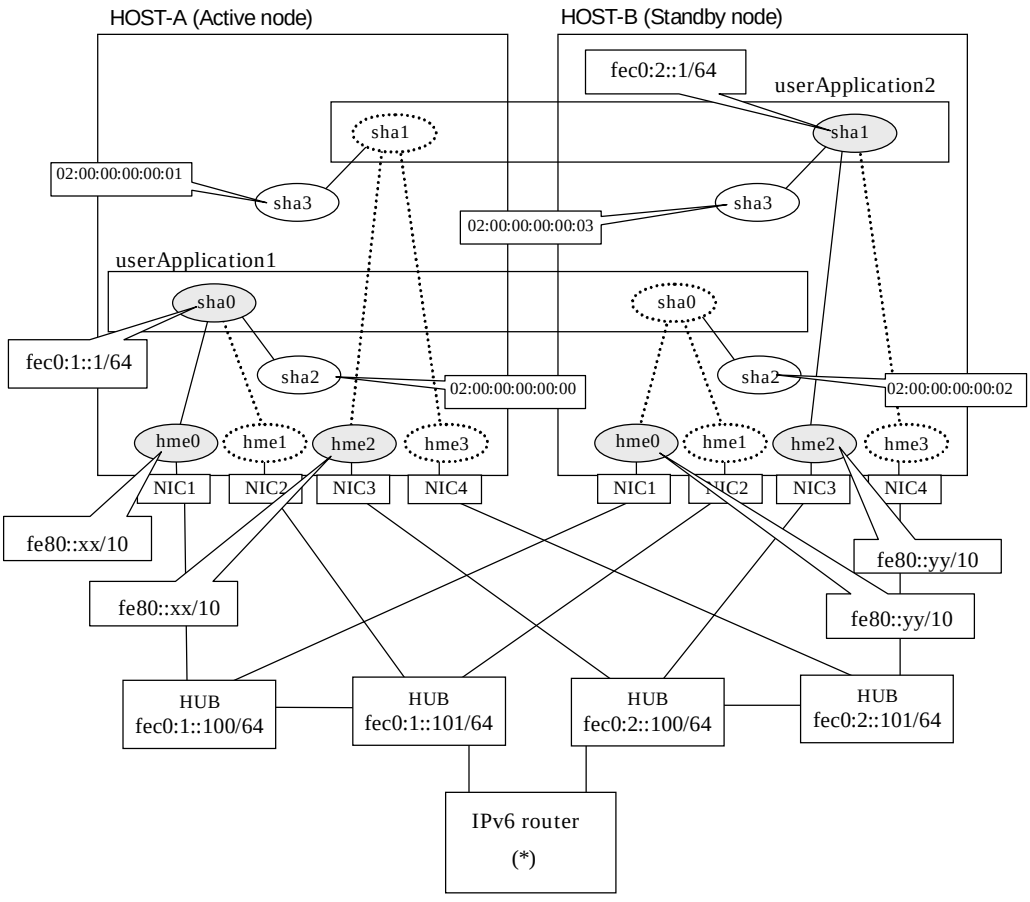
The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

```
ifdefault AdvSendAdvertisements true   # Every interface sends a router advertisement.
prefix fec0:1::0/64 hme0               # hme0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 hme2               # hme2 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme2 files as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta         # HOST-A/B Takeover virtual IP (1)
fec0:1::100     swhub1            # Primary HUB IP (1)
fec0:1::101     swhub2            # Secondary HUB IP (1)
fec0:2::1       v6hostb         # HOST-A/B Takeover virtual IP (2)
fec0:2::100     swhub3            # Primary HUB IP (2)
fec0:2::101     swhub4            # Secondary HUB IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme2 are enabled as IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t hme2,hme3
```

4) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100,fec0:2::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -a 02:00:00:00:00:01 -t sha1
```

6) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

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

8) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha2
/opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 and /etc/hostname6.hme2 files as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme2 are enabled as IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t hme2,hme3
```

4) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100,fec0:2::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -a 02:00:00:00:00:03 -t sha1
```

6) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

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

8) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha2
/opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::1” and “fec0:2::1”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.7.8 Example of the Cluster system (Mutual standby) with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

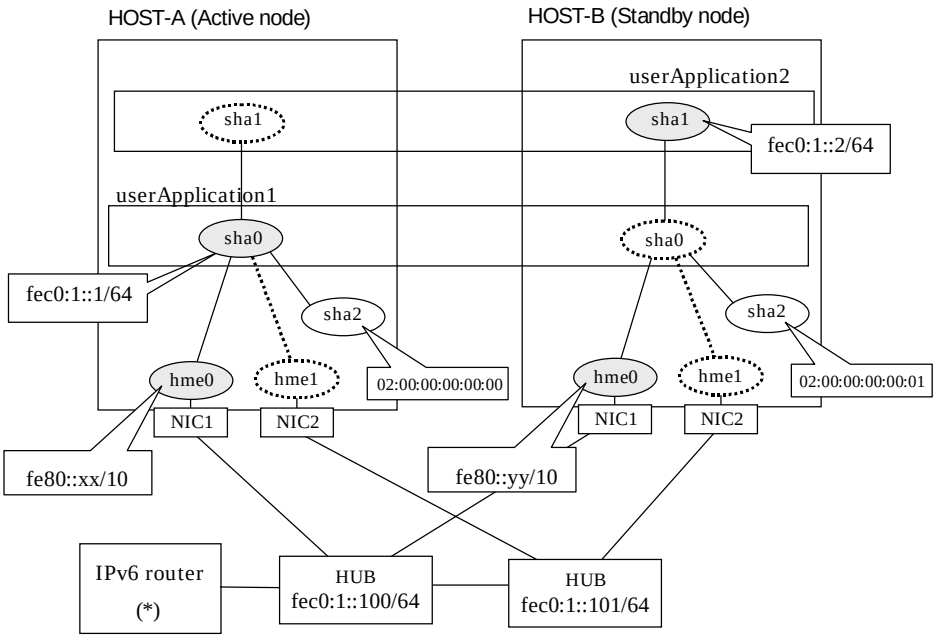
The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta         # HOST-A/B Takeover virtual IP (1)
fec0:1::2       v6hostb         # HOST-A/B Takeover virtual IP (2)
fec0:1::100     swhub1            # Primary HUB IP
fec0:1::101     swhub2            # Secondary HUB IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0

6) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha2

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

5) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0
```

6) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

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

8) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::1” and “fec0:1::2”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.7.9 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

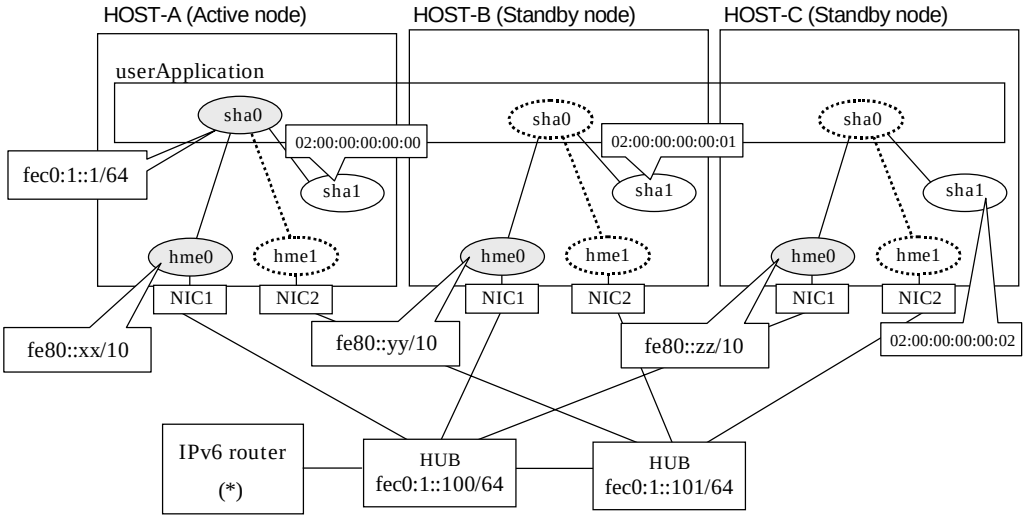
The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1       v6hosta          # HOST-A/B/C Takeover virtual IP
fec0:1::100     swhub1             # Primary HUB IP
fec0:1::101     swhub2             # Secondary HUB IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-C]

1) Setting up the system

1-1) Create /etc/hostname6.hme0 file as an empty file.

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

4) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off

5) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:02 -t sha0

6) Creation of takeover virtual interface

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

7) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

8) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-B and HOST-C, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C.
Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address “fec0:1::1”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.8 Example of configuring NIC switching mode (IPv4/IPv6)

When using IPv6 address, it is required to set an IPv6 router on the same network. Also, specify the same prefix and prefix length of IPv6 address for redundant control line function configured in the IPv6 router.

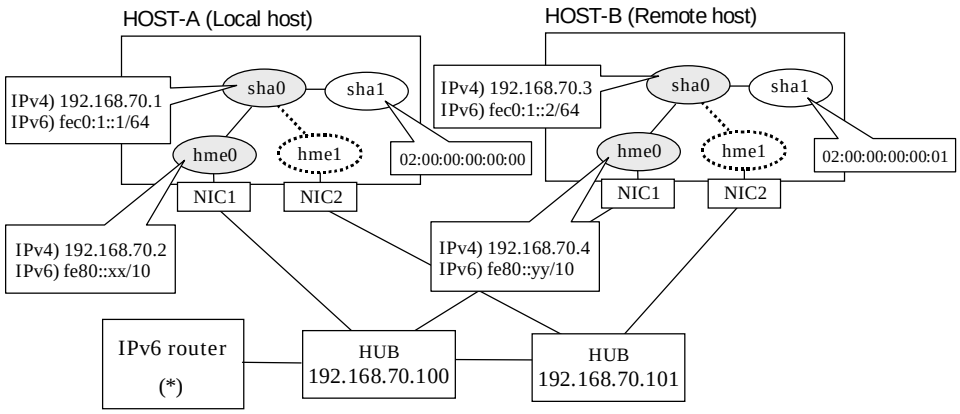
B.8.1 Example of the Single system without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A Virtual IP
192.168.70.2      host11    # HOST-A Physical IP
192.168.70.3      hostb     # HOST-B Virtual IP
192.168.70.4      host21    # HOST-B Physical IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1         v6hosta     # HOST-A Virtual IP
fec0:1::2         v6hostb     # HOST-B Virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

7) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

7) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

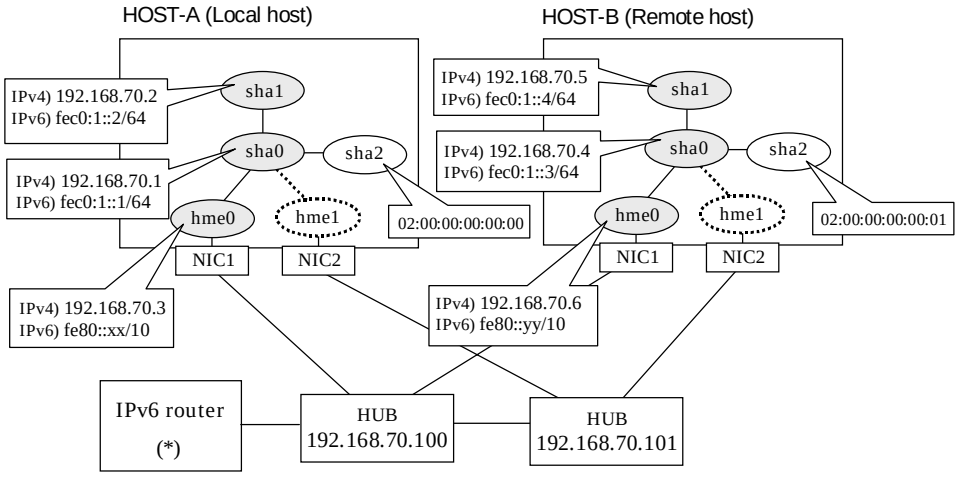
B.8.2 Example of the Single system with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta1   # HOST-A Virtual IP (1)
192.168.70.2      hosta2   # HOST-A Virtual IP (2)
192.168.70.3      host11   # HOST-A Physical IP
192.168.70.4      hostb1   # HOST-B Virtual IP (1)
192.168.70.5      hostb2   # HOST-B Virtual IP (2)
192.168.70.6      host21   # HOST-B Physical IP
192.168.70.100    swhub1   # Primary HUB IP
192.168.70.101    swhub2   # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1         v6hosta1     # HOST-A Virtual IP (1)
fec0:1::2         v6hosta2     # HOST-A Virtual IP (2)
fec0:1::3         v6hostb1     # HOST-B Virtual IP (1)
fec0:1::4         v6hostb2     # HOST-B Virtual IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1
/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/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0

7) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t hme0,hme1
/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/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0

7) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

8) Starting the HUB monitoring function

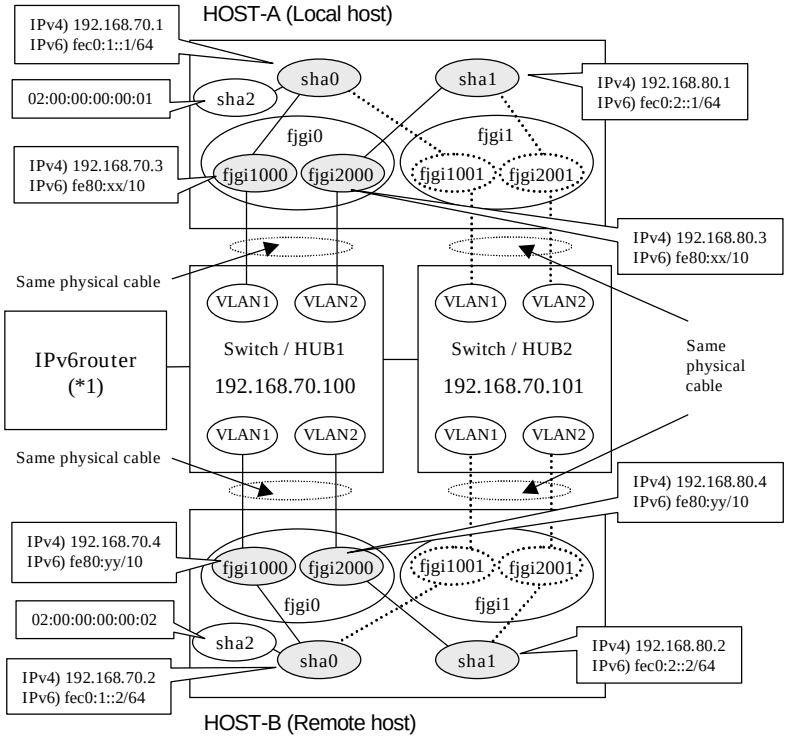
/opt/FJSVhanet/usr/sbin/hanetpoll on

B.8.3 Configuring virtual interfaces with tagged VLAN (synchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

```
ifdefault AdvSendAdvertisements true    # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi1000            # fjgi1000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi2000            # fjgi2000 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.3    host71   # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1    hostb    # HOST-A Virtual IP
192.168.80.3    host81   # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2    hostc    # HOST-B Virtual IP
```

```
192.168.70.4      host72    # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2      hostd     # HOST-B Virtual IP
192.168.80.4      host82    # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100    swhub1     # primary Switch/HUB IP
192.168.70.101    swhub2     # secondary Switch/HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host71
```

- Contents of /etc/hostname.fjgi2000

```
host81
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
192.168.80.0      255.255.255.0
```

1-4) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2000 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1         v6hosta1    # HOST-A Virtual IP(1)
fec0:2::1         v6hosta2    # HOST-A Virtual IP(2)
fec0:1::2         v6hostb1    # HOST-B Virtual IP(1)
fec0:2::2         v6hostB2     # HOST-B Virtual IP(2)
```

2) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t fjgi2000,fjgi2001
```

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.fjgi2000.

3) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::1/64
```

4) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

5) Setting up the HUB monitoring function (Synchronized switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

6) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0
```

7) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2000 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host72
```

- Contents of /etc/hostname.fjgi2000

```
host82
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2000 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t fjgi2000,fjgi2001
```

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.2000.

3) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::2/64
```

4) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

5) Setting up the HUB monitoring function (Synchronized switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

6) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0
```

7) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2000 are enabled as IPv4/IPv6 interfaces after rebooting the system.

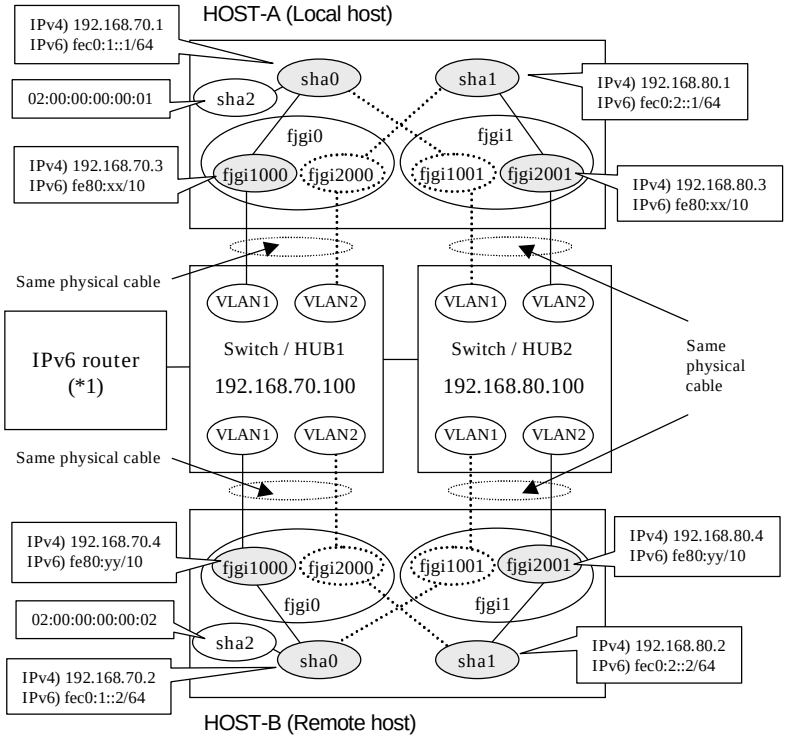
```
/usr/sbin/shutdown -y -i6 -g0
```

B.8.4 Configuring virtual interfaces with tagged VLAN (asynchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

```
ifdefault AdvSendAdvertisements true    # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi1000            # fjgi1000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi2001            # fjgi2001 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.3    host71   # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1    hostb    # HOST-A Virtual IP
192.168.80.3    host81   # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2    hostc    # HOST-B Virtual IP
```

```
192.168.70.4      host72    # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2      hostd     # HOST-B Virtual IP
192.168.80.4      host82    # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100    swhub1     # Switch/HUB1 IP
192.168.80.100    swhub2     # Switch/HUB2 IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host71
```

- Contents of /etc/hostname.fjgi2001

```
host81
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
192.168.80.0      255.255.255.0
```

1-4) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2001 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1         v6hosta1    # HOST-A Virtual IP(1)
fec0:2::1         v6hosta2    # HOST-A Virtual IP(2)
fec0:1::2         v6hostb1    # HOST-B Virtual IP(1)
fec0:2::2         v6hostB2     # HOST-B Virtual IP(2)
```

2) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t fjgi2001,fjgi2000
```

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.fjgi2001.

3) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::1/64
```

4) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0
```

6) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2001 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi1000

```
host72
```

- Contents of /etc/hostname.fjgi2001

```
host82
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.fjgi1000 and /etc/hostname6.fjgi2001 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t fjgi1000,fjgi1001
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t fjgi2001,fjgi2000
```

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi1000 and /etc/hostname.fjgi2001.

3) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::2/64
```

4) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:02 -t sha0
```

6) Reboot

Run the following command to reboot the system. Make sure fjgi1000 and fjgi2001 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

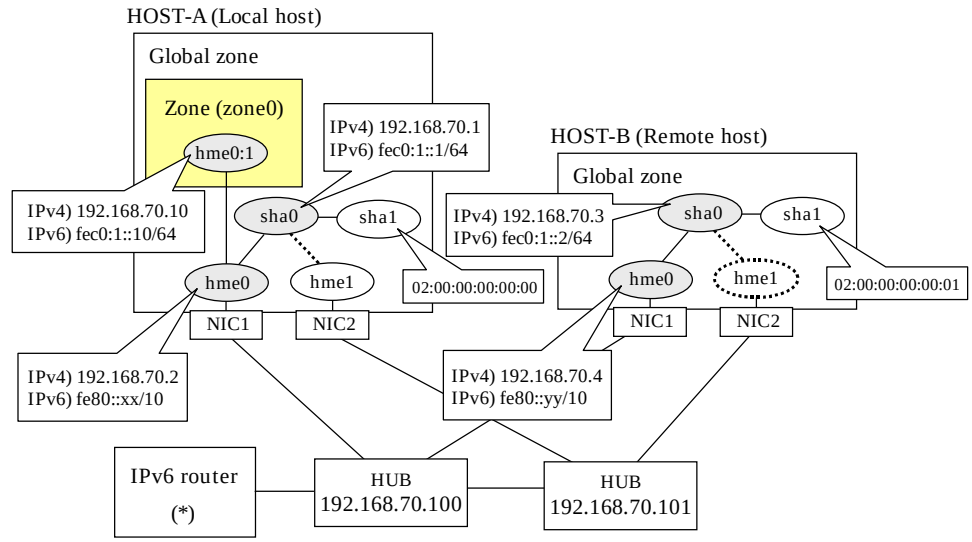
B.8.5 Network configuration in the Solaris container (logical IP takeover)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta      # HOST-A Virtual IP
192.168.70.2      host11     # HOST-A Physical IP
192.168.70.3      hostb      # HOST-B Virtual IP
192.168.70.4      host21     # HOST-B Physical IP
192.168.70.100    swhub1     # Primary HUB IP
192.168.70.101    swhub2     # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1         v6hosta     # HOST-A Virtual IP
fec0:1::2         v6hostb     # HOST-B Virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:00 -t sha0

7) Change the method of deactivating the standby interface

/opt/FJSVhanet/usr/sbin/hanetparam -d plumb

8) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

9) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

10) Set up a zone

Set up a zone by executing the following command:

/usr/sbin/zonecfg -z zone0

10-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

10-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in NIC switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.70.10
zonecfg:zone0:net> set physical=hme0
zonecfg:zone0:net> end
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=hme0
zonecfg:zone0:net> end
```

The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.
If you specify the redundant physical interface in NIC switching mode, specify the primary physical interface.

10-3) Check the above setting.

```
zonecfg:zone0> export
```

10-4) Check setup consistency.

```
zonecfg:zone0> verify
```

10-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

11) Install the zone

Install the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 install

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

12) Start up the zone

Start up the zone by executing the following command:

/usr/sbin/zoneadm -z zone0 boot

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

7) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

B.8.6 Example of the Cluster system (1:1 Standby) without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

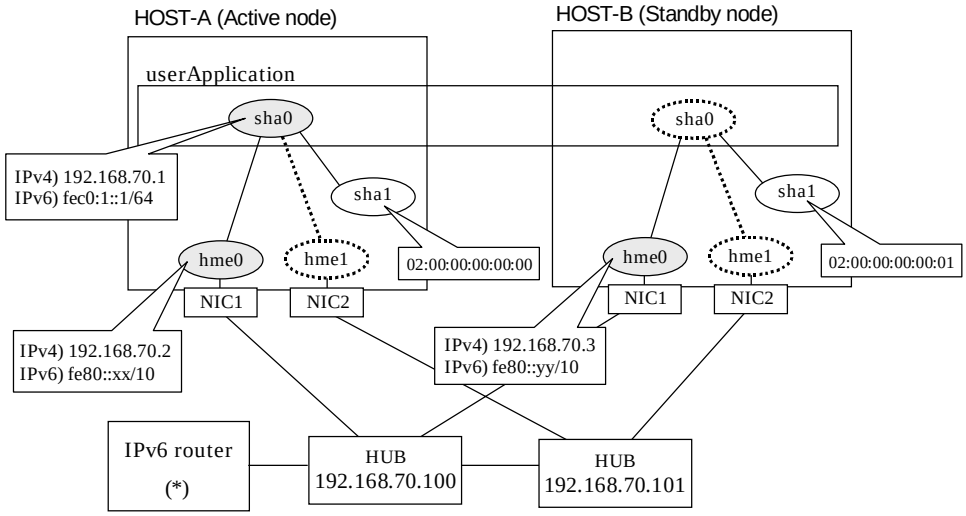
The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B Takeover virtual IP
192.168.70.2      host11    # HOST-A Physical IP
192.168.70.3      host21    # HOST-B Physical IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1          v6hosta1     # HOST-A/B Takeover virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

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 -a 02:00:00:00:00:00 -t sha0

7) Creation of takeover virtual interface

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

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

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 -a 02:00:00:00:00:01 -t sha0

7) Creation of takeover virtual interface

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

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resource, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover

address “192.168.70.1 - fec0:1::1”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.8.7 Example of the Cluster system (Mutual Standby) without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

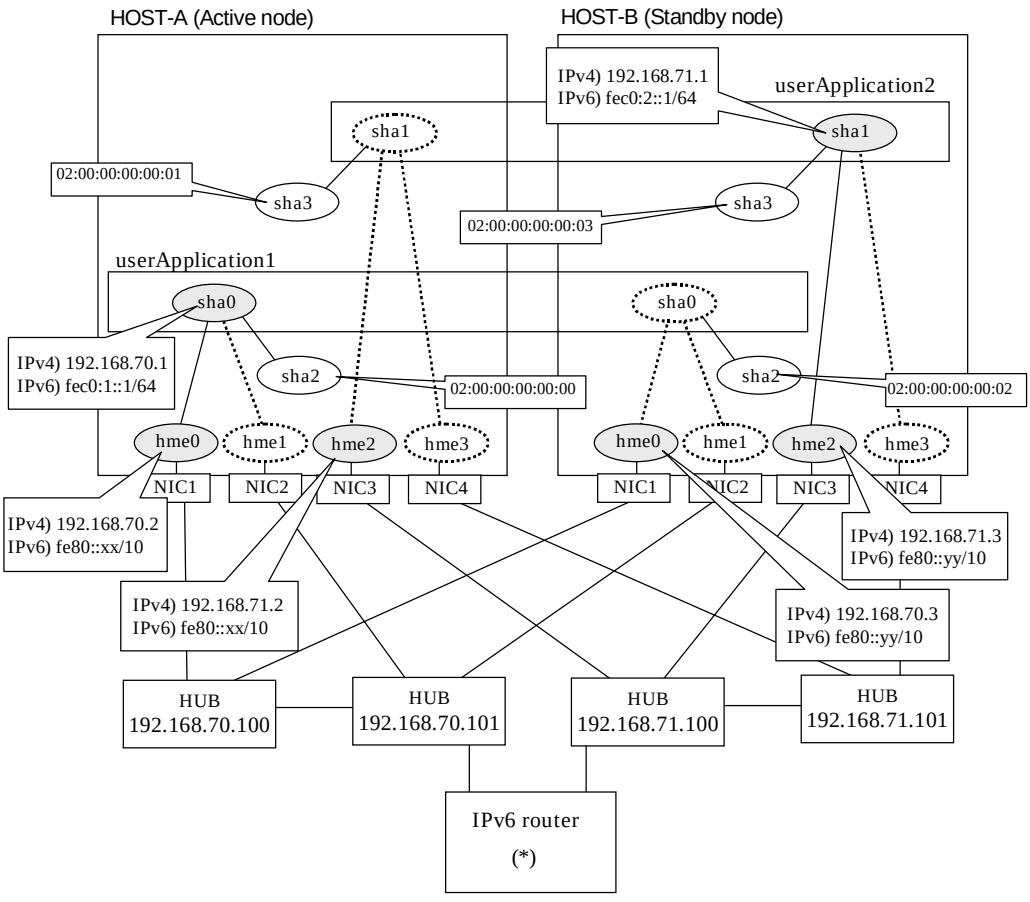
The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

```
ifdefault AdvSendAdvertisements true   # Every interface sends a router advertisement.
prefix fec0:1::0/64 hme0               # hme0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 hme2               # hme2 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1     hosta    # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2     host11   # HOST-A Physical IP (1)
192.168.70.3     host21   # HOST-B Physical IP (1)
192.168.71.1     hostb    # HOST-A/B Virtual IP (Takeover IP2)
192.168.71.2     host12   # HOST-A Physical IP (2)
192.168.71.3     host22   # HOST-B Physical IP (2)
192.168.70.100   swhub1   # Primary HUB IP (1)
192.168.70.101   swhub2   # Secondary HUB IP (1)
192.168.71.100   swhub3   # Primary HUB IP (2)
192.168.71.101   swhub4   # Secondary HUB IP (2)
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

- Contents of /etc/hostname.hme2

```
host12
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0     255.255.255.0
192.168.71.0     255.255.255.0
```

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme2 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1        v6hosta     # HOST-A/B Takeover virtual IP (1)
fec0:2::1        v6hostb     # HOST-A/B Takeover virtual IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme2 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t hme2,hme3

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0 and /etc/hostname.hme2.

4) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t hme2,hme3
```

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 -a 02:00:00:00:00:00 -t sha0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -a 02:00:00:00:00:01 -t sha1
```

7) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

8) Starting the HUB monitoring function

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

9) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha2
/opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

- Contents of /etc/hostname.hme2

```
host22
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 and /etc/hostname6.hme2 files as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 and hme2 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t
hme2,hme3
```

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0 and /etc/hostname.hme2.

4) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t hme2,hme3
```

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 -a 02:00:00:00:00:02 -t sha0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -a 02:00:00:00:00:03 -t sha1
```

7) Creation of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

8) Starting the HUB monitoring function

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

9) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha2
/opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1 - fec0:1::1” and “192.168.71.1 - fec0:2::1”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.8.8 Example of the Cluster system (Mutual Standby) with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

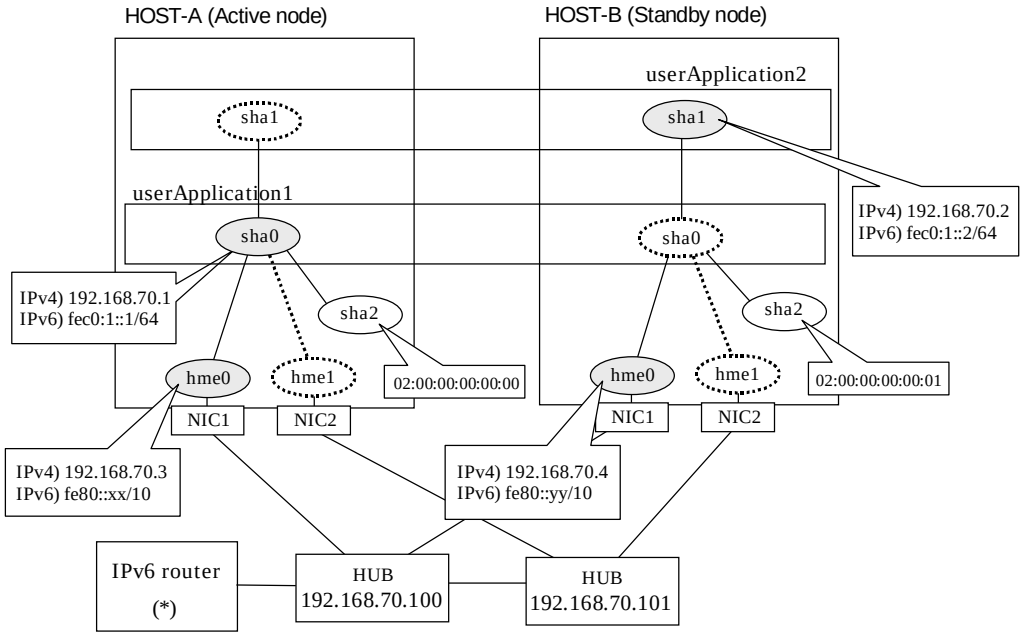
The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta     # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2      hostb     # HOST-A/B Virtual IP (Takeover IP2)
192.168.70.3      host11    # HOST-A Physical IP
192.168.70.4      host21    # HOST-B Physical IP
192.168.70.100    swhub1    # Primary HUB IP
192.168.70.101    swhub2    # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1         v6hosta      # HOST-A/B Takeover virtual IP (1)
fec0:1::2         v6hostb      # HOST-A/B Takeover virtual IP (2)
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1
/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/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:00 -t sha0

7) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha2

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t hme0,hme1
/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/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64

5) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1

6) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -a 02:00:00:00:00:01 -t sha0

7) Creation of takeover virtual interface

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha2

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A and HOST-B. Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1 - fec0:1::1” and “192.168.70.2 - fec0:1::2”.

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.8.9 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

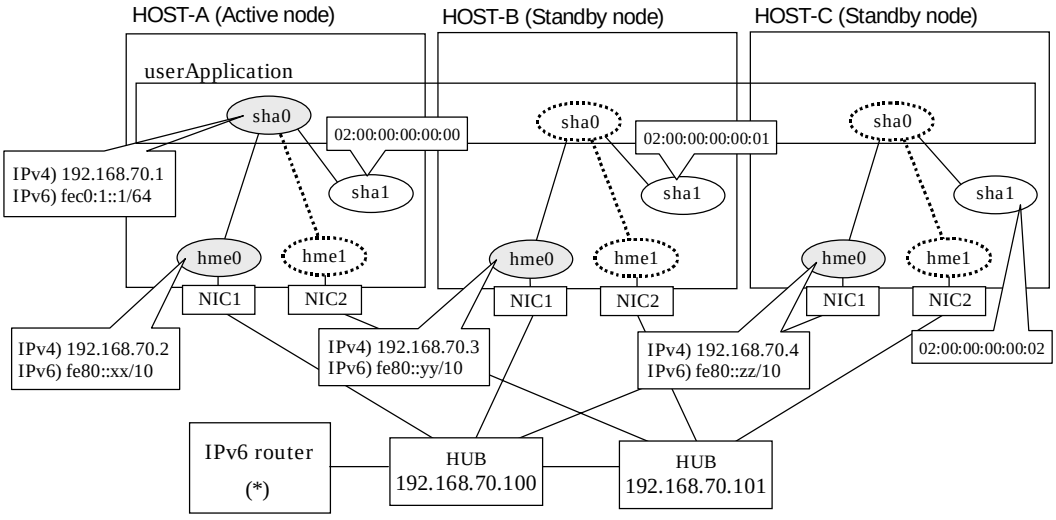
The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to “D.2 Trouble shooting”.



Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

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

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1      hosta      # HOST-A/B/C Takeover virtual IP
192.168.70.2      host11     # HOST-A Physical IP
192.168.70.3      host21     # HOST-B Physical IP
192.168.70.4      host31     # HOST-C Physical IP
192.168.70.100    swhub1     # Primary HUB IP
192.168.70.101    swhub2     # Secondary HUB IP
```

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host11
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0      255.255.255.0
```

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1          v6hosta1          # HOST-A/B/C Takeover virtual IP
```

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

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 -a 02:00:00:00:00:00 -t sha0

7) Creation of takeover virtual interface

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

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host21
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

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 -a 02:00:00:00:00:01 -t sha0

7) Creation of takeover virtual interface

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

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.hme0

```
host31
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/hostname6.hme0 file as an empty file.

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure hme0 are enabled as IPv4/IPv6 interfaces after rebooting the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of IPv4 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t hme0,hme1

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.hme0.

4) Creation of IPv6 virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

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 -a 02:00:00:00:00:02 -t sha0

7) Creation of takeover virtual interface

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

8) Starting the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll on

9) Starting the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/strptl -n sha1

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-B and HOST-C, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C.
Once Gls is created, register the two Gls resources on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address “192.168.70.1 - fec0:1::1”.

2) Starting of userApplication

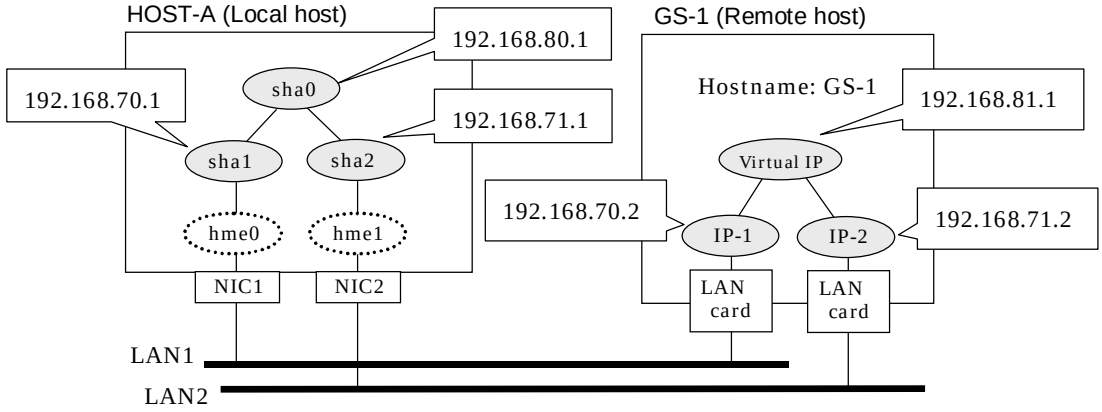
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.9 Example of configuring GS/SURE linkage mode

B.9.1 Example of the Single system in GS/SURE connection function (GS communication function)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the GS, refer to the GS manual.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Virtual IP (mode:n)
192.168.71.1    host12   # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta    # HOST-A Virtual IP (mode:c)
192.168.70.2    gs11      # GS-1 Physical IP (1)
192.168.71.2    gs12      # GS-1 Physical IP (2)
192.168.81.1    gsa       # GS-1 Virtual IP
```

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Reboot

Run the following command and reboot the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2

4) Setting the Communication target monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.2,192.168.71.2 -m on
```

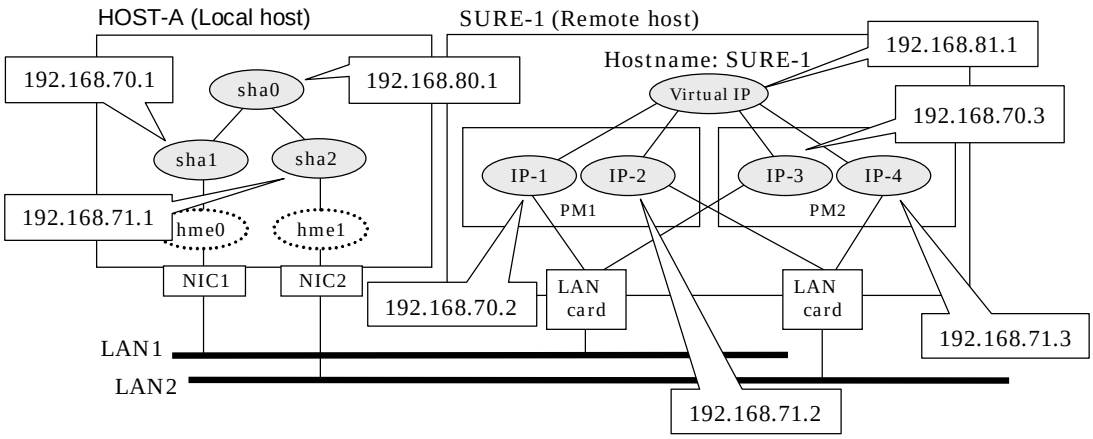
5) Activation of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

B.9.2 Example of the Single system in GS/SURE connection function (SURE communication function)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the SURE, refer to the SURE manual.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Virtual IP (mode:n)
192.168.71.1    host12   # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta    # HOST-A Virtual IP (mode:c)
192.168.70.2    sure11   # SURE-1 Physical IP (1)
192.168.71.2    sure12   # SURE-1 Physical IP (2)
192.168.70.3    sure13   # SURE-1 Physical IP (3)
192.168.71.3    sure14   # SURE-1 Physical IP (4)
192.168.81.1    surea    # SURE-1 Virtual IP (1)
192.168.81.2    sureb    # SURE-1 Virtual IP (2)
```

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Reboot

Run the following command and reboot the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2

4) Setting the Communication target monitoring function

/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t
192.168.70.2:1,192.168.71.2:1,192.168.70.3:2,192.168.71.3:2 -m on -r on

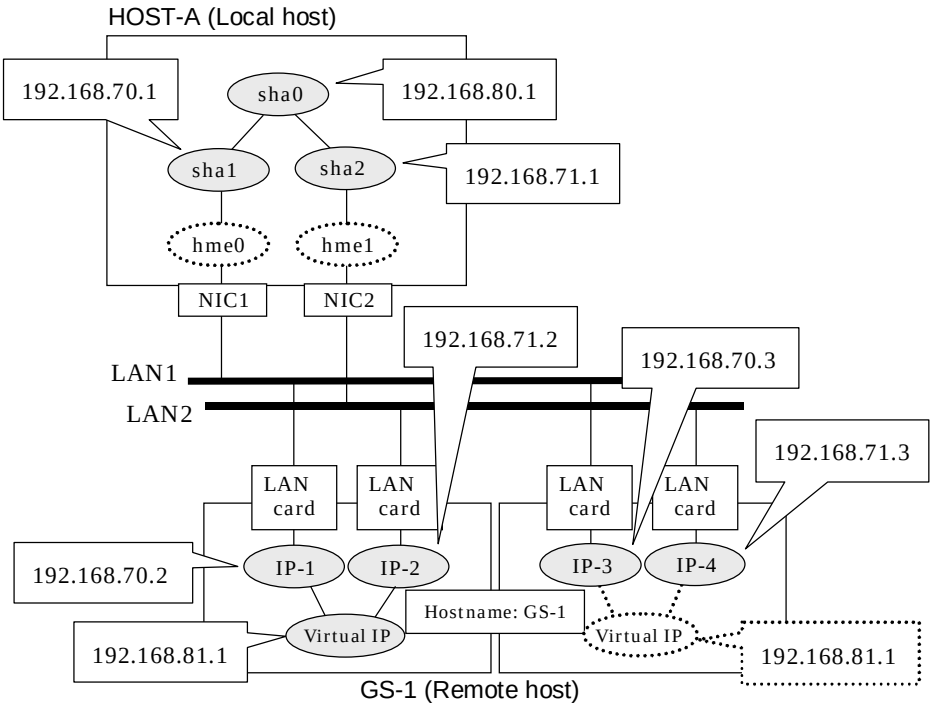
5) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.9.3 Example of the Single system in GS/SURE connection function (GS Hot-standby)

This section describes an example of configuring an environment for GS Hot-standby.

For configuring the GS, refer to the GS manual.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Virtual IP (mode:n)
192.168.71.1    host12   # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta    # HOST-A Virtual IP (mode:c)
192.168.70.2    gs11      # GS-1 Physical IP (1)
192.168.71.2    gs12      # GS-1 Physical IP (2)
192.168.70.3    gs13      # GS-1 Physical IP (3)
192.168.71.3    gs14      # GS-1 Physical IP (4)
192.168.81.1    gsa       # GS-1 Virtual IP
```

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Reboot

Run the following command and reboot the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

4) Setting the Communication target monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.2,192.168.71.2 -m on
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.3,192.168.71.3
```

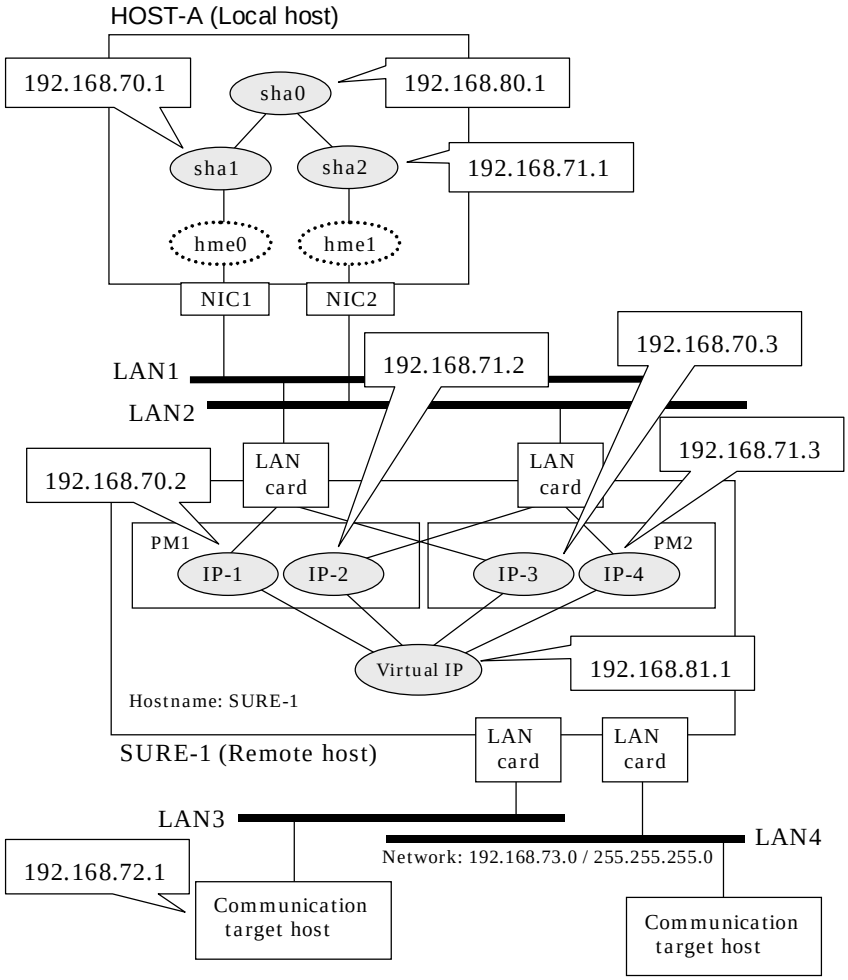
5) Activation of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

B.9.4 Example of the Single system in TCP relay function

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the SURE, refer to the SURE manual.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Virtual IP (mode:n)
192.168.71.1    host12   # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta    # HOST-A Virtual IP (mode:c)
192.168.70.2    sure11   # SURE-1 Physical IP (1)
192.168.71.2    sure12   # SURE-1 Physical IP (2)
192.168.70.3    sure13   # SURE-1 Physical IP (3)
192.168.71.3    sure14   # SURE-1 Physical IP (4)
192.168.81.1    surea    # SURE-1 Virtual IP (1)
192.168.81.2    sureb    # SURE-1 Virtual IP (2)
```

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

192.168.71.0	255.255.255.0
192.168.80.0	255.255.255.0
192.168.81.0	255.255.255.0

2) Reboot

Run the following command and reboot the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2

4) Setting the Communication target monitoring function

/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t
192.168.70.2:1,192.168.71.2:1,192.168.70.3:2,192.168.71.3:2 -m on -r on

5) Setting the TCP relay function

/opt/FJSVhanet/usr/sbin/hanetobserv create -i 192.168.81.1 -c
192.168.72.1,192.168.73.0:255.255.255.0

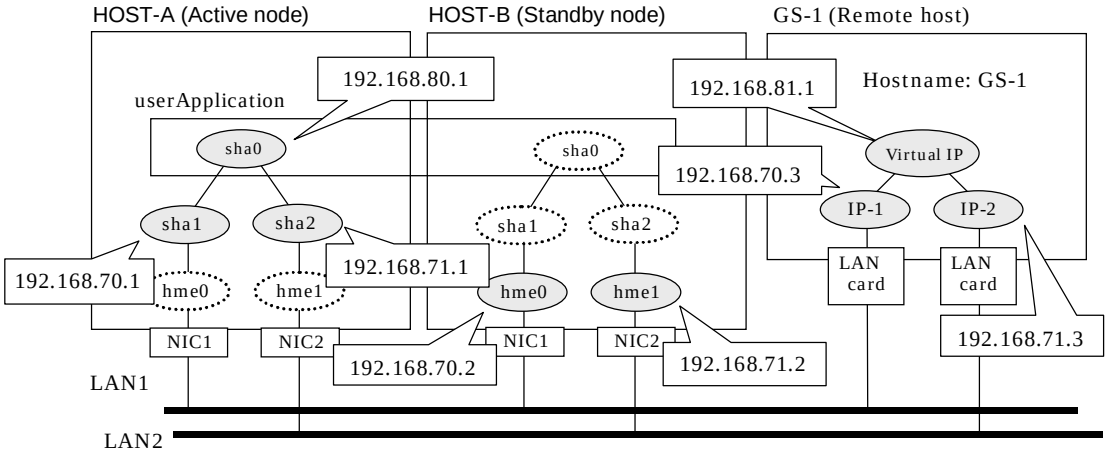
6) Activation of virtual interface

/opt/FJSVhanet/usr/sbin/strhanet

B.9.5 Example of the Cluster system in GS/SURE connection function (GS communication function)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the GS, refer to the GS manual.
For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Virtual IP (mode:n)
192.168.71.1    host12   # HOST-A Virtual IP (mode:n)
192.168.70.2    host21   # HOST-B Virtual IP (mode:n)
192.168.71.2    host22   # HOST-B Virtual IP (mode:n)
192.168.80.1    hosta    # HOST-A/B Virtual IP (mode:c, Takeover virtual IP)
192.168.70.3    gs11      # GS-1 Physical IP (1)
192.168.71.3    gs12      # GS-1 Physical IP (2)
192.168.81.1    gsa       # GS-1 Virtual IP
```

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Reboot

Run the following command and reboot the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.3,192.168.71.3 -m on -r on
```

Setting the Standby node monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.80.1 -t
192.168.70.2,192.168.71.2 -m on -r on
```

When configuring standby node monitoring information, it is necessary to specify the takeover IP address for '-i' option.

5) Creation of takeover virtual interface

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

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command and reboot the system.

```
/usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.2 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.2 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.3,192.168.71.3 -m on -r on
```

Setting the Active node monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.80.1 -t
192.168.70.1,192.168.71.1 -m on -r on
```

When configuring active node monitoring information, it is necessary to specify the takeover IP address for '-i' option.

5) Creation of takeover virtual interface

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

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 5) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resource, select the SysNode for HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address “192.168.80.1”.

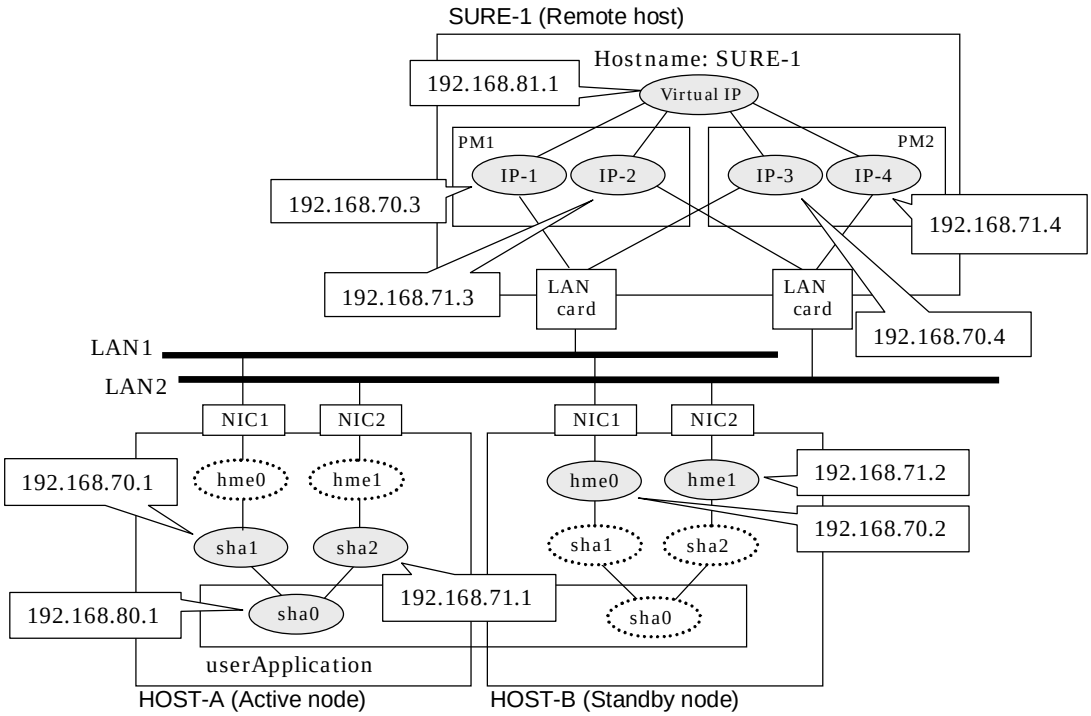
2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.9.6 Example of the Cluster system in GS/SURE connection function (SURE communication function)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the SURE, refer to the SURE manual.
For configuring the cluster system, refer to the Cluster system manual.
In this section, description of private LAN is omitted.
The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11   # HOST-A Virtual IP(mode:n)
192.168.71.1    host12   # HOST-A Virtual IP(mode:n)
192.168.70.2    host21   # HOST-B Virtual IP(mode:n)
192.168.71.2    host22   # HOST-B Virtual IP(mode:n)
192.168.80.1    hosta    # HOST-A/B Virtual IP(mode:c, Takeover virtual IP)
192.168.70.3    sure11   # SURE-1 Physical IP(IP-1)
192.168.71.3    sure12   # SURE-1 Physical IP(IP-2)
192.168.70.4    sure13   # SURE-1 Physical IP(IP-3)
192.168.71.4    sure14   # SURE-1 Physical IP(IP-4)
192.168.81.1    surea    # SURE-1 Virtual IP
```

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Reboot

Run the following command and reboot the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t 192.168.70.3:1,192.168.71.3:1,192.168.70.4:2,192.168.71.4:2 -m on -r on

Setting the Standby node monitoring information:

/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.80.1 -t 192.168.70.2,192.168.71.2 -m on -r on

When configuring standby node monitoring information, it is necessary to specify the takeover IP address for '-i' option.

5) Creation of takeover virtual interface

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

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Create /etc/notrouter file as an empty file.

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command and reboot the system.

/usr/sbin/shutdown -y -i6 -g0

3) Creation of virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.2 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.2 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t 192.168.70.3:1,192.168.71.3:1,192.168.70.4:2,192.168.71.4:2 -m on -r on

Setting the Active node monitoring information:

/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.80.1 -t 192.168.70.1,192.168.71.1 -m on -r on

When configuring active node monitoring information, it is necessary to specify the takeover IP address for '-i' option.

5) Creation of takeover virtual interface

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

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.
To create Gls resource, select the SysNode for HOST-A and HOST-B. Once Gls is created, register it on the userApplication.
When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

Appendix C Changes from previous versions

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

C.1 Changes from Redundant Control Line function 4.0 to version 4.1A10

Table C.1 is a list of changes made from the previous version.

Table C.1 List of changes from Redundant Control Line function 4.0 to 4.1A10.

Incompatible type	Subject	Affected version
Incompatible commands	hanetbackup command	PRIMECLUSTER GLS 4.1A10 or later
	hanetrestore command	PRIMECLUSTER GLS 4.1A10 or later

C.1.1 A list of new commands

There is no new command for redundant control line function 4.1A10.

C.1.2 A list of incompatible commands

The followings are the incompatible commands of redundant control line function from the previous version. In addition, please refer to "Chapter 7 Command reference" about the details of each command.

C.1.2.1 hanetbackup command

[Contents]

Now, it is possible to backup the configuration file without taking package version into account.

[Changes]

Before modification

The user must keep in track on which version of the backup configuration files belong to.

After modification

When restoring backup configuration files, the user is not required to know the version of the backup configuration files.

C.1.2.2 hanetrestore command

[Contents]

Now, it is possible to restore the configuration file without taking package version into account.

[Changes]

Before modification

The user must keep in track on which version of the backup configuration files belong to.

After modification

When restoring backup configuration files, the user is not required to know the version of the backup configuration files.

[Notes]

- For the configuration files on Redundant Line Control function 4.1A10, the user is still not required to know the version of the backup configuration files when restoring the backup configuration files.

C.2 Changes from Redundant control function 4.1A10 to version 4.1A20

Table C.2 is a list of changes made from the previous version.

Table C.2 List of changes from Redundant Control Line function 4.1A10 to 4.1A20.

Incompatible type	Subject	Affected version
Incompatible commands	hanetconfig command	PRIMECLUSTER GLS 4.1A20 or later
	hanetpoll command	PRIMECLUSTER GLS 4.1A20 or later
	hanetobserv command	PRIMECLUSTER GLS 4.1A20 or later
Incompatible functionalities	Default GLS resource value on the standby node of the cluster system.	PRIMECLUSTER GLS 4.1A20 or later
	Interface state monitoring feature.	PRIMECLUSTER GLS 4.1A20 or later

C.2.1 A list of new commands

There are no new commands for redundant control line function 4.1A20.

C.2.2 A list of incompatible commands

In Redundant Line Control function 4.1A20, the following commands are incompatible commands from the previous versions. In addition, please refer to "Chapter 7 Command reference" about the details of each command.

C.2.2.1 hanetconfig command

[Contents]

If a host name you specify via 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 4.1A10 contains host name written in characters other than alphanumeric, period or hyphen, delete these characters. The virtual interface cannot be activated if the host name contains characters other than alphanumeric, period or hyphen.

C.2.2.2 hanetpoll command

[Contents]

If a host name you specify via 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 4.1A10 contains host name written in characters other than alphanumeric, period or hyphen, delete these characters. The virtual interface cannot be activated if the host name contains characters other than alphanumeric, period or hyphen.

C.2.2.3 hanetobserv command

[Contents]

If a host name you specify via hanetobserv 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 "7.5 hanetobserv Command".

[Changes]

Before modification

Invalid characters were not treated as an error.

After modification

Invalid characters were treated as an error.

[Notes]

- When migrating the backup configuration setting file to 4.1A20, if the backup configuration settings file (created via hanetbackup command) prior to 4.1A10 contains host name written in characters other than alphanumeric, period or hyphen, delete these characters. The virtual interface cannot be activated if the host name contains characters other than alphanumeric, period or hyphen.

C.2.3 Other incompatibles

C.2.3.1 Resource state monitoring function for standby node

[Contents]

When creating cluster application, it is possible to convert standby node of GLS resource into "Standby" state by setting a value of "Standby Transition" attribute. If neglecting this configuration, it will not monitor the status of standby node of GLS resource. For reference, see "5.1.4 Monitoring resource status of standby node".

[Changes]

Before modification

GLS resource is set to "Offline" and it does not monitor the standby node of GLS resource state.

After modification

GLS resource is converted as "Standby" status and it monitors the standby node of GLS resource status.

[Notes]

- For GS/SURE linkage mode, the virtual interface on standby node side is inactive and its monitoring function stops. Therefore, it cannot monitor the GLS resource on the standby node. Unlike other modes, GS/SURE linkage mode does not require to specify “StandbyTransition” attribute because it does not run the resource monitoring.
- When attempting to restore the configuration file for 4.1A10 to the cluster system of

version 4.1A20 or later using the backup function of a cluster system, the value "StandbyTransistion" attribute will not be set as the default value. If this configuration is used without any modification, it does not monitor the GLS resource status in standby node. In such case, temporary stop the cluster application and use Admin View to apply the "StandbyTransition" attribute in the configuration file.

C.2.3.2 Interface state 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 runnning. For details on interface state monitoring function, refer to "2.3.4 Interface state 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 "7.15 resethanet Command".

C.3 Changes from Redundant control function 4.1A20 to version 4.1A30

Table C.3 is a list of changes made from the previous version.

Table C.3 List of changes from Redundant Control Line function 4.1A20 to 4.1A30.

Incompatible type	Subject	Affected version
Incompatible commands	hanetconfig command	PRIMECLUSTER GLS 4.1A30 or later
	hanetpoll command	PRIMECLUSTER GLS 4.1A30 or later
	strhanet command	PRIMECLUSTER GLS 4.1A30 or later
	stphanet command	PRIMECLUSTER GLS 4.1A30 or later
	dsppoll command	PRIMECLUSTER GLS 4.1A30 or later
Incompatible features	Activation timing of GS/SURE Linkage mode on the cluster system.	PRIMECLUSTER GLS 4.1A30 or later
	Verifying the Network address	PRIMECLUSTER GLS 4.1A30 or later

C.3.1 A list of new commands

There are no new commands for redundant control line function 4.1A30.

C.3.2 A list of incompatible commands

In Redundant Line Control function 4.1A30, the following commands are incompatible commands from the previous versions. In addition, please refer to "Chapter 7 Command reference" about the details of each command.

C.3.2.1 hanetconfig command

[Contents]

Dynamic expansion/modification/deletion is allowed by the command while operating Redundant Line Control function.

[Changes]

Before modification

System reboot reflects configured values, which were added, modified, or deleted during the operation.

After modification

The configured value will be effective immediately after the configuration values were added, modified, or deleted during the operation.

C.3.2.2 hanetpoll command

[Contents]

Starting or stopping the polling process of each virtual interface as well as configuration or display of polling is allowed for the HUB monitoring function on NIC Switching mode.

[Changes]

Before modification

If there were multiple virtual interfaces, starting or stopping polling and configuring/displaying configuration values could not be achieved individually.

Configuration parameters of multiple virtual interfaces would look like the following.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
 Polling Status         = OFF
         interval(idle) =   5( 60) sec
         time           =   5 times
         max_retry      =   5 retry
         repair_time    =   5 sec
 FAILOVER Status        = YES
 Name    HUB Poll Hostname
+-------+--------+-----------------------------------------------------+
 sha0       OFF   swhub1,swhub2
 sha1       ON    swhub3,swhub4
```

After modification

Now it is possible to start or stop polling and configure or display the configuration values of each virtual interface in the case where multiple virtual interfaces are present.

Configuration parameters of multiple virtual interfaces would look like the following.

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

[ Polling Parameter of each interface ]
 Name    Hostname/Polling Parameter
+-------+-----------------------------------------------------------------+
 sha0    swhub1,swhub2
         hub-hub poll       =    OFF
         interval(idle)     =      5( 60) sec
         times              =      5 times
         max_retry          =      5 retry
         repair_time        =      5 sec
         failover mode      =    YES

 Name    Hostname/Polling Parameter
+-------+-----------------------------------------------------------------+
 sha1    swhub3,swhub4
         hub-hub poll       =     ON
         interval(idle)     =      5( 60) sec
         times              =      5 times
         max_retry          =      5 retry
         repair_time        =      5 sec
         failover mode      =    YES
```

[Notes]

- No modification is applied to polling feature of RIP mode and GS/SURE Linkage mode.

C.3.2.3 strhanet command

[Contents]

If there is more than one virtual interface failed to activate when attempting to activate the virtual interface, error messages will be produced according to the number of virtual interfaces encountered the failure.

[Changes]

Before modification

This command did not generate an error message for every virtual interface.

The following message will be displayed when enabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0,sha1
hanet: 00000: information: normal end.
```

After modification

Now, this command generates an error message for every virtual interface.

The following message will be displayed when enabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0,sha1
hanet: 00000: information: normal end. name=sha0
hanet: 00000: information: normal end. name=sha1
```

[Notes]

- You can verify which virtual interface has encountered a failure while running the command.

C.3.2.4 stphanet command

[Contents]

If there is more than one virtual interface failed to inactivate when attempting to inactivate the virtual interface, error messages will be produced according to the number of virtual interfaces encountered the failure.

[Changes]

Before modification

This command did not generate an error message for every virtual interface.

The following message will be displayed when disabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0,sha1
hanet: 00000: information: normal end.
```

After modification

Now, this command generates an error message for every virtual interface.

The following message will be displayed when disabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0,sha1
hanet: 00000: information: normal end. name=sha0
hanet: 00000: information: normal end. name=sha1
```

[Notes]

- You can verify which virtual interface has encountered a failure while running the command.

C.3.2.5 dsppoll command

[Contents]

This command displays polling information of each virtual interface on Router/HUB monitoring function. This command only displays polling parameters of one virtual interface.

[Changes]

Before modification

This command did not display the polling parameters of each virtual interface.

The polling status would be displayed as follows.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
 Polling Status    =  ON
 inter(idle)       =   5( 60)
 times             =   5
 retry             =   5
 repair_time       =   5
 FAILOVER Status   =  YES

 Status  Name  Mode Primary Target/Secondary Target            HUB-HUB
+------+------+----+-----------------------------------------+-------+
   ON   sha0    d   swhub1(ON)/swhub2(WAIT)                    OFF
   ON   sha1    d   swhub3(ON)/swhub4(WAIT)                   ACTIVE
```

After modification

Now, this command displays the polling parameters of each virtual interface.

The polling status would be displayed as follows.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
+------+-------------------------------------------------------------------------+
 sha0   Polling Status    =     ON
        Primary Target(status)   = swhub1(ON)
        Secondary Target(status) = swhub2(WAIT)
        HUB-HUB status    =    OFF
        interval(idle)    =      2( 60)   times            =      3
        repair_time       =      5        retry            =      5
        FAILOVER Status   =    YES
+------+-------------------------------------------------------------------------+
 sha1   Polling Status    =     ON
        Primary Target(status)   = swhub3(ON)
        Secondary Target(status) = swhub4(WAIT)
        HUB-HUB status    = ACTIVE
        interval(idle)    =      4( 60)   times            =      5
        repair_time       =      5        retry            =      5
        FAILOVER Status   =    YES
+------+-------------------------------------------------------------------------+

# /opt/FJSVhanet/usr/sbin/dsppoll -n sha0

 Polling Status    =  ON
 interval          =   2
 idle              =  60
 times             =   3
 retry             =   5
 repair_time       =   5
 failover mode     = YES
 Status  Name  Mode Primary Target/Secondary Target            HUB-HUB
+------+------+----+-----------------------------------------+-------+
   ON   sha0    d   swhub1(ON)/swhub2(WAIT)                    OFF
```

[Notes]

- If you are using an application that references the output of dsppoll command, you must be aware that the output will be different. However, adding '-n' command allows outputting the polling parameter of each virtual interface in the same format before the modification.
- In the case of displaying polling target's parameters using '-c' option (as it has been the usual way of displaying the polling parameter), there are no changes made.

C.3.3 Other incompatibles

C.3.3.1 Activation timing of GS/SURE Linkage mode on the Cluster System

[Contents]

On an environment where GS/SURE Linkage mode is operating on the cluster system, activate a standby node of a virtual interface (operation mode 'n') from the system startup.

[Changes]

Before modification

During the system starts up, the virtual interface on standby node (operation mode 'n') will not be activated. Instead, the physical interface will be activated.

After modification

During the system starts up, the virtual interface on standby node (operation mode 'n') will be activated. But, the physical interface will not be activated.

[Notes]

- The interface name activated on standby node turns into virtual interface names, such as not physical interface names, such as "hmeX", but "shaX" etc.

C.3.3.2 Verifying the Network address

[Contents]

During system configuration or activation of virtual interfaces, Redundant Line Control function now verifies for the consistency of network address for configured virtual IP address and physical IP address. In the case where invalid network address of virtual or physical IP address are configured, it will output the following warning.

Warning:

hanet: 35800: warning: the same network addresses are inappropriate.

Before the hanetconfig command defines virtual interfaces, please define sub-net mask as a /etc/inet/netmasks file. A warning message may be outputted when sub-net mask is not being defined in advance.

[Changes]

Before modification

It did not check for the consistency of network address for the configured IP addresses.

Network Address	Redundant Mode	Results	
Network address of each interface (physical interface, virtual interface, etc.) is consistent	NIC Switching mode	Valid configuration	No warning message
	Fast Switching mode	Invalid configuration	
	RIP mode		
	GS/SURE linkage mode		

After modification

Verifies for the consistency of network address for the configured IP addresses.

Network Address	Redundant Mode	Results	
Network address of each interface (physical interface, virtual interface, etc.) is consistent	NIC Switching mode	Invalid configuration	No warning message
	Fast Switching mode	Valid configuration	Outputs warning message (No.358)
	RIP mode		
	GS/SURE linkage mode		

[Notes]

- If warning message (No.358) displays while running the following commands, check the IP address or net mask value configured on the physical and virtual interfaces. It is possible that IP address or net mask value is invalid. Note that, command process continues execution regardless of the warning messages.
  - /opt/FJSVhanet/usr/sbin/hanetconfig create
  - /opt/FJSVhanet/usr/sbin/hanetconfig modify
  - /opt/FJSVhanet/usr/sbin/hanetconfig copy
  - /opt/FJSVhanet/usr/sbin/strhanet
  - /opt/FJSVhanet/usr/sbin/hanetnic add
  - /opt/FJSVhanet/usr/sbin/hanethvrsc create
- When the definition error of a network address is detected at the time of system starting or RMS starting, a warning message may be outputted to syslog instead of a standard error (stderr).

C.4 Changes from Redundant control function 4.1A30 to version 4.1A40

Table C.4 is a list of changes made from the previous version.

Table C.4 List of changes from Redundant Control Line function 4.1A30 to 4.1A40

Incompatible type	Subject	Affected version
Incompatible commands	None	-
Incompatible features	Check for consistency between Solaris container and network configuration	PRIMECLUSTER GLS 4.1A40 or later
	Reserve takeover virtual interface for fast switching mode	PRIMECLUSTER GLS 4.1A40 or later

C.4.1 A list of new commands

There are no new commands for redundant control line function 4.1A40.

C.4.2 A list of incompatible commands

No commands in the redundant line control function 4.1A40 are incompatible from the previous versions.

C.4.3 Other incompatibles

C.4.3.1 Check for consistency between Solaris container and network configuration

[Contents]

If the Solaris zone is already set on the system in fast switching or NIC switching mode, check consistency between the Solaris container and network configuration.

If one of the following warning messages is output during environment settings, it is necessary to check the network configuration in the Solaris container.

Messages:

hanet: 36301: warning: IP address is already defined in zones. zone=<zone_name>
hanet: 36401: warning: interface name is defined in zones. zone=<zone_name>
hanet: 36501: warning: secondaryIF is specified in zones. zone=<zone_name>

For corrective action against each message, see "A.1.2 Error output message (numbers 100 to 500)".

[Changes]

Before modification

The network configuration in the Solaris container is not recognized.

After modification

Consistency between the Solaris container and network configuration is checked.

[Notes]

- Consistency between the Solaris container and network configuration will be checked regardless of zone startup or stop if the zone is already set on the system.
- Consistency between the Solaris container and network configuration will not be checked if the network is configured first then the zone is set on the system.

C.4.3.2 Reserve takeover virtual interface for fast switching mode

[Contents]

If the virtual interface in fast switching is registered as a cluster takeover resource with the "hanethvrsc" command, it will use the logical ID No.65 or later like "shaX:65" and "shaX:66".

If the virtual interface in fast switching is specified for multiple zones, the logical ID will be the same as that for the takeover virtual interface. However, the logical virtual interfaces like "shaX:65" and "shaX:66" will be generated in advance when the redundant line control function is started then the cluster takeover virtual interface will automatically be reserved. So, the same logical ID will not be used for multiple zones, and the cluster takeover virtual interface can be used.

[Changes]

Before modification

When the virtual interface and takeover IP are set with the "hanethvrsc" command, the takeover virtual interfaces like shaX:65 and shaX:66 will not be reserved.

See the following output example of the "ifconfig" command after the virtual interface and takeover IP settings.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
2
        inet 192.168.100.10 netmask ffffff00 broadcast 192.168.100.255
        ether XX:XX:XX:XX:XX:XX
hme1: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
3
        inet 192.168.101.10 netmask ffffff00 broadcast 192.168.101.255
        ether XX:XX:XX:XX:XX:XX
hme2: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
4
        inet 192.168.102.10 netmask ffffff00 broadcast 192.168.102.255
        ether XX:XX:XX:XX:XX:XX
cip0: flags=10080c1<UP,RUNNING,NOARP,PRIVATE,IPv4> mtu 1500 index 6
        inet 192.168.1.1 netmask ffffff00
sha0: flags=1000863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4>
mtu 1500 index 8
        inet 192.168.200.10 netmask ffffff00 broadcast 192.168.200.255
        ether XX:XX:XX:XX:XX:XX
```

After modification

When the virtual interface and takeover IP are set with the "hanethvrsc" command, the takeover virtual interfaces like shaX:65 and shaX:66 will automatically be reserved.

See the following output example of the "ifconfig" command after the virtual interface and takeover IP settings.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
```

```
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
2
        inet 192.168.100.10 netmask ffffff00 broadcast 192.168.100.255
        ether XX:XX:XX:XX:XX:XX
hme1: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
3
        inet 192.168.101.10 netmask ffffff00 broadcast 192.168.101.255
        ether XX:XX:XX:XX:XX:XX
hme2: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
4
        inet 192.168.102.10 netmask ffffff00 broadcast 192.168.102.255
        ether XX:XX:XX:XX:XX:XX
cip0: flags=10080c1<UP,RUNNING,NOARP,PRIVATE,IPv4> mtu 1500 index 6
        inet 192.168.1.1 netmask ffffff00
sha0: flags=1000863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4>
mtu 1500 index 8
        inet 192.168.200.10 netmask ffffff00 broadcast 192.168.200.255
        ether XX:XX:XX:XX:XX:XX
sha0:65: flags=1000862<BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4>
mtu 1500 index 8
        inet 0.0.0.0 netmask 0
```

The "ifconfig" command outputs the takeover virtual interface (sha0:65). The environment settings and operation of a cluster system are the same as before.

[Notes]

- When a cluster takeover virtual interface is registered, it will be reserved regardless of availability of zones.
- The generated takeover virtual interface is "down", and "0.0.0.0" is allocated to the IP address. The takeover IP address is allocated during RMS startup then the interface will be "up".

Appendix D Notice of supplemental information

This appendix provides supplemental information regarding GLS.

D.1 Changing Methods of Activating and Inactivating Interface

This section describes how to activate or deactivate network interfaces controlled through redundant line control.

D.1.1 INTERSTAGE Traffic Director and Solaris container

If you use "INTERSTAGE Traffic Director" or Solaris container for upper layers in NIC switching, it is necessary to change the method of deactivating standby physical interfaces by executing the following command:

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d plumb
```

If you stop the "INTERSTAGE Traffic Director" or Solaris container, return the method of activating or deactivating the interfaces.

To return the method of deactivating the standby physical interfaces, execute the following command:

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d unplumb
```

The setting value is enabled when

- the system is rebooted,
- the virtual interfaces are deactivated or activated
- NIC is switched

The changed value will be enabled in all the virtual interfaces in NIC switching.

D.2 Trouble shooting

The cause of the frequently occurred trouble when using a Redundant Line Control function and how to deal with it are explained in this section.

D.2.1 Communication as expected cannot be performed (Common to IPv4 and IPv6)

D.2.1.1 A default gateway is not set valid

Phenomenon:

A default gateway defined in /etc/defaultrouter at activation of a system is not valid.

Cause and how to deal with:

The setting of a default gateway defined in /etc/defaultrouter is set in /etc/rc2.d/S69inet at activation of a system. At this time, when an interface of the same segment as that of the specified router, or when not activated, it is not possible to set a default gateway. In a Redundant Line Control function, a virtual interface is activated at activation of a userApplication in cluster operation. Therefore, occasionally not possible to set a default gateway.

Fast switching mode:

When using a virtual interface as a sending interface to a default gateway in cluster operation, change the timing to activate a virtual interface by a hanetparam command.

RIP mode:

It is not possible to user a virtual interface as a sending interface to a default gateway in cluster operation.

NIC switching mode:

When using a physical IP address takeover function, and also when not activating an interface in a standby node, it is not possible to use a physical interface as a sending interface to a default gateway.

GS/SURE linkage mode:

It is not possible to use a virtual interface as a sending interface to a default gateway in cluster operation.

D.2.1.2 The route information set by a route command is deleted

Phenomenon:

The static route information set by a route add command is deleted.

Cause and how to deal with:

In a Redundant Line Control function, when activating and deactivating an interface, or when detected an error in a transfer route, the route information is flushed and in.routed is reactivated if necessary. At this time, the static route information set by a route command is deleted.
When using in.routed, necessary to define the static route information in /etc/gateways. For instance, to set the route information to a specific network (suppose network: 192.13.80.0, gateway address: 192.13.70.254, and metric value: 3), /etc/gateways is described as follows:

```
net 192.13.80.0 gateway 192.13.70.254 metric 3 passive
```

D.2.1.3 Fails to activate a system or an interface in the NIS environment

Phenomenon:

The following message is displayed and activation of a system or an interface hangs up.

```
ypbind[xxxx]: [ID xxxxxx daemon.error] NIS server not responding for domain
"domain_name"; still trying
```

Cause and how to deal with:

When a system that a Redundant Line Control function works is set as an NIS client, occasionally not possible to connect NIS server temporarily due to the process to deactivate an interface executed by a Redundant Line Control function. In such a case, if set a netmask to an interface by an ifconfig command, occasionally the process to activate a system or an interface hangs up because an ifconfig command waits for the connection with NIS server to get a subnet mask.
Be sure to set as follows when using a Redundant Line Control function in the NIS environment.

To specify "files" first in /etc/nsswitch.conf to refer "netmasks".

[Example of setting]

```
netmasks: files
```

or

```
netmasks: files [NOTFOUND=return] nis
```

As to accessing NIS server, design a network not to use an interface that is the target of control in a Redundant Line Control function (activation/deactivation) as possible.

D.2.1.4 Automatic address configuration lags behind for IPv6

Phenomenon:

Automatic stateless address configuration for IPv6 may not operate instantly when activating IPv6. As a consequence, it takes time to add site-local/global addresses.

Cause and how to deal with:

When activating an interface for IPv6, a link-local address is added to the physical interface to activate the physical interface. To instantly create site-local/global address by the automatic stateless address configuration, it transmits the "router solicitation message" to the adjacent router to request for router advertisement message from the router. However, once the interface activates, if spanning tree protocol (STP) is running on the HUB, it takes time to hold a communication. Thus it may fail to request router advertisement messages. Because IPv6 router transmits the router advertisement message periodically and automatic stateless address automatic configuration runs after certain amount of time, it is possible to hold a communication of site-local/global addresses. Nevertheless, if the time interval parameter of transmitting the router advertisement message is set for a considerably long time, it may consume a long time until the automatic stateless address configuration starts and to hold a communication. In such case, either establish a link for operation NIC and standby NIC or modify the router setting so that a router transmits the router advertisement message within a fewer minutes interval.

D.2.2 Virtual interface or the various functions of Redundant Line Control function cannot be used

D.2.2.1 An interface of NIC switching mode is not activated

Phenomenon:

The following message is output and activation of an interface fails.

```
hanet: ERROR: 85700: polling information is not defined. Devname = sha0(0)
```

Cause and how to deal with:

In NIC switching mode, switching interfaces inside a node and between nodes is controlled using a failure monitoring function. Therefore, NIC switching mode does not work only by defining the information of a virtual interface using a hanetconfig create command. Necessary to set the monitor-to information by a hanetpoll create command. When the monitor-to information is not set, a takeover IP address is not activated either. Activation of a userApplication fails in cluster operation.
When using a logical address takeover function, and also when sharing a physical interface, necessary to have the monitor-to information in a unit of information of each virtual interface. In such a case, duplicate the information of a virtual interface and the monitor-to information that defined initially using a hanetconfig copy command and a hanetpoll copy command.

D.2.2.2 It does not failback at the time of the restoration detection by standby patrol in NIC switching mode

Phenomenon:

The following messages display during recovering process of standby patrol in NIC switching mode. As a result, it fails to instantly switch back from the secondary interface to the primary interface.

```
hanet: INFO: 88500: standby interface recovered. (sha1)
hanet: INFO: 89700: immediate exchange to primary interface is canceled. (sha1)
```

Cause and how to deal with:

After switching from the primary interface to the secondary interface due to transfer path failure, if a standby patrol recovers prior to elapsed link up delay time (default is 60 sec), the switching process between the primary and secondary interface may loop infinitely. To prevent from this symptom, the above messages will display to stop the switching process for the primary interface. The main reason of covering this issue in this section is to prevent infinite loop of switching interfaces when setting routes for monitoring and instead of HUBs.

D.2.2.3 Error detection message displays for standby patrol in NIC switching mode

Phenomenon:

The following message is output and activation of an interface fails.

```
hanet: WARNING: 87500: standby interface failed.
```

Cause and how to deal with:

On the network where VLAN switch exists on the transfer path monitored via standby patrol function, this error occurs if the following two circumstances take place:

1) Connecting a redundant NIC to a port of disparate VLAN identifier.
2) Connecting one of a redundant NIC or both redundant NICs to tagged member port of the switch.

The VLAN switch cannot communicate in between the ports where VLAN identifiers are disparate. Therefore, when connecting redundant NIC to disparate VLAN identifier, transmitting the monitoring frame fails between standby NIC and operation NIC, consequentially outputting 875 message. Additionally, even if VLAN identifiers are the same port and this port is set to tag member, and in the condition where the NIC does not support tag 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 tag VLAN, set the port of the switch as non-tag member.

D.2.2.4 Command aborts and Redundant Line Control function startup fails

Symptom

Executing hanetconfig create/delete command, hanetpoll create/delete command, dsphanet command, and dsppoll commands output the following error message and aborts. Also, the virtual interface fails to activate during the system startup.
“hanet: 56100: internal error: daemon process does not exist.”

Cause and workaround

The problem is most likely occurred due to cut off of symbolic link that was linked to initialization script for Redundant Line Control function. The user might have performed illegal operation to generate this issue. Therefore, the initialization script of Redundant Line Control function did not run during the system startup in which have caused activation failure of the virtual interface as well as startup failure of GLS daemon (hanetcltd). In such a case, the command also aborts since the GLS daemon is not running.
To resolve this issue, refer to the following recovery procedure to create the symbolic link under /etc/rc2.d and /etc/rc3.d that links to the initialization script and reboot the system.

[Recovery Procedure]

```
# ln -s /etc/init.d/hanet /etc/rc2.d/S32hanet
# ln -s /etc/init.d/hanet99 /etc/rc3.d/S99hanet
```

D.2.2.5 Unable to establish connection using virtual IP address of GS/SURE Linkage mode

Symptom

Fails to establish connection using a virtual IP address on GS/SURE Linkage mode due to routing daemon startup failure during the system startup.

Cause and workaround

On Solaris 8 or Solaris 9, if /etc/defaultrouter file does not exist, it runs /usr/sbin/in.rdisc(1M) to implement reference process by RDISC (router search protocol). If a router on the network is running RDISC, it uses RDISC as the routing protocol instead of RIP, preventing /usr/sbin/in.routed(1M) from startup. This issue can be resolved by changing the name of /usr/sbin/in.rdisc file (for example,/usr/sbin/in.rdisc.saved) to disable RDISC reference process.

If this problem occurs on Solaris 10, change the setting as /usr/sbin/in.routed(1M) can be executed as a routing daemon by executing /usr/sbin/routeadm(1M).
For details on this issue, refer to the Solaris manual.

How to detect this symptom:

Your system is having this problem if all of the followings are found.

Solaris 8 or Solaris 9:
1) /etc/notrouter file (empty file) exists
2) /etc/defaultrouter file exists.
3) Routing daemon (/usr/sbin/in.routed) does not exist after system startup.
4) Routing table contains the default path.

Solaris 10:
1) The routing daemon is set in "/usr/sbin/in.rdisc" through /usr/sbin/routeadm(1M).
2) Routing daemon (/usr/sbin/in.routed) does not exist after system startup.
3) Routing table contains the default path.

Detecting routing daemon

If /usr/sbin/in.routed process name appears when running the following command, the routing daemon process is running.

```
# ps -ef | grep in.routed
```

Detecting the default path

You can check for the default path by running the following command. If a word "default" is displayed under "Destination", the default path is present.

```
# netstat -rn | grep default
default                192.168.70.254          UG            1          1    hme0
```

D.2.2.6 Solaris container cannot be started

Symptom

If the virtual interface in fast switching or physical interface in NIC switching is specified for the network setting, the following error message will be output and zone startup will fail:

```
# zoneadm -z zone0 boot
could not verify net address=192.168.80.10 physical=sha0: No such device or
address
zoneadm: zone zone0 failed to verify
```

or

```
# zoneadm -z zone0 boot
zoneadm: zone 'zone0': hme0:1: could not bring interface up: address in use by zone
'global': Cannot assign requested address
zoneadm: zone 'zone0': call to zoneadmd failed
```

Cause and workaround

If the specified interface does not exist in the zone network setting or the IP address same as that specified for the zone network setting, the zone cannot be started. Check if the specified interface or IP address already exists using the "ifconfig(1M)" command.
If you are using NIC switching, check if the method of deactivating the standby interface can be used in the zone. For details, see "7.6 hanetparam Command" and "D.1 Changing Methods of Activating and Inactivating Interface".

- If a zone is installed, and interfaces for the zone do not exist, zone installation will fail. You need to activate the interfaces specified for the zone network settings before zone installation.

D.2.3 Failure occurs during operation (Common to both Single and Cluster system)

D.2.3.1 Switching takes place in NIC switching mode regardless of failure at the monitoring end

Phenomenon:

Even though there is no error in network devices, the following message is output and HUB monitoring ends abnormally.

```
hanet: ERROR: 87000: polling status changed: primary polling failed.
(hme0,target=192.13.71.20)
hanet: ERROR: 87100: polling status changed: secondary polling failed.
(hme1,target=192.13.71.21)
```

Cause and how to deal with:

In NIC switching mode, 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 ping 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.

```
link up latency > STP transfer delay time * 2 + monitoring period * number of monitoring
```

- To operate ping monitoring over the system that runs firewall, configure the firewall so that ping can pass through the firewall. Otherwise, it fails to operate ping monitoring. The firewall settings must be the same for both of the primary and secondary interfaces.

D.2.3.2 Takes time to execute an operation command or to activate a userApplication

Phenomenon:

Takes time to execute an operation command of a Redundant Line Control function.
Takes time to activate a userApplication or to switch nodes at the cluster operation.

Cause and how to deal with:

When a host name or an IP address specified in the information of a virtual interface, the monitor-to information, etc. is not described in /etc/inet/hosts file, or when "files" are not specified at the top in an address solution of /etc/nsswitch.conf, occasionally it takes time to process an internally executed name-address conversion. Therefore, it takes time to execute a command, or for the cluster state to change. Check that all IP addresses and host names to use in a Redundant Line Control function are described in /etc/inet/hosts, and that /etc/inet/hosts is referred first at name-address conversion.

D.2.3.3 TCP connection is not divided in GS/SURE linkage mode

Phenomenon:

Even though TCP communication by a virtual IP is executed in GS/SURE linkage mode, the number of the connections is not shown when displayed how the connection is divided using a dsphanet command.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -c
  Name   IFname Connection
 +------+------+----------+
 sha0   sha2        -
        sha1        -
 sha10  sha12       -
        sha11       -
```

Cause and how to deal with:

When dividing TCP connection in GS/SURE linkage mode, necessary to define the information of the other system with a hanetobserv command. Any protocol other than TCP is not divided. UDP and ICMP are sent according to the route information.

D.2.4 Failure occurs during operation (In the case of a Cluster system)

D.2.4.1 Node switching is not executed in Fast switching mode

Phenomenon:

Failover between clusters (job switching between nodes) is not executed in Fast switching mode at cluster operation.

Cause and how to deal with:

In Fast switching mode, it is decided that an error occurred in a transfer route when a response from all other systems in communication was cut off. Therefore, node switching is not executed when all cables are pulled out or when the power of all HUBs is not turned on. When the following message is often displayed, check the cables or HUBs.

```
unix: NOTICE: SUNW,hme1: No response from Ethernet network : Link Down - cable problem?
```

D.2.5 Failure occurs when using IPv6 address (Common to both Single and Cluster system)

D.2.5.1 Automatic address configuration malfunctions while using standby interface in NIC switching mode

Phenomenon:

If IPv6 virtual interface for NIC switching mode is used on the system operating as an IPv6 router, automatic stateless address configuration in the corresponding network ceases to function after switching the interface in the node. As a result, it cannot hold a communication with site-local/global address.

Cause and how to deal with:

In order to use IPv6 virtual interface for NIC switching mode in the system operating as an IPv6 router, both operation and standby NIC must contain the same configuration information in /etc/inet/ndpd.conf configuration file.

The following is an example of /etcinet/ndpd.conf under situation in which operation NIC is hme1, standby NIC is hme2, and distributed network prefix is fec0:1::0/64.

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

D.2.6 Failure occurs while using IPv6 address (In the case of a Cluster system)

D.2.6.1 Fails to activate IPv6 takeover address

Phenomenon:

Outputs the following message and fails to activate IPv6 takeover IP address.

```
ifconfig: Duplicate address detected on link hme1 for address fec0:1380::100. Code 1
```

Cause and how to deal with:

If an IPv6 address is overlapping with the other systems, when attempting to activate an interface, the address overlap detection function causes to stop the activation of a takeover IP address. Be sure to check the other systems for over lapping IP addresses.

D.2.7 Resuming connection lags after switching (Common to both Single and Cluster system)

D.2.7.1 Recovery of transmission falls behind after switching to standby interface in NIC switching mode

Phenomenon:

When switching interface from operation NIC to standby NIC in NIC switching mode where HUB in the network is running Spanning Tree Protocol (STP), it takes roughly 30 seconds to hold a communication with standby NIC.

Cause and how to deal with:

In the HUB where STP is running, establishing link by activating an interface does not necessary mean to acquire communication instantly. In such environment, after a link has established on the port where NIC is connected, transmitting data is temporary constrained by transmission delay timer (Forward-time). In order to establish a communication instantly after switching to standby NIC, use the standby patrol. Standby patrol establishes a link regularly in both operation and standby NIC, so that the transmitting data would not be constrained by transmission delay timer (Forward-time) of STP.

D.2.8 Resuming connection lags after switching (In the case of a Cluster system)

D.2.8.1 Resuming connection of IP takeover address takes time after switching node

Phenomenon:

When manually switching a node while communicating with other system, it takes time to resume the connection of IPv6 takeover address.

Cause and how to deal with:

After performing takeover process of IPv6 between the nodes, the remote system primary connected to the node cannot instantly identify the Link-Layer Address for IPv6 takeover address. As a consequence, it takes approximately 30 seconds to enable a connection. To prevent such case, start in.ripngd (IPv6 routing daemon) beforehand in both operation and standby nodes to attain a connection instantly. A packet transmitted from the remote system is sent to Link-Layer Address of the primary node. This packet is being relayed from the primary node over to the new node while it reports the ICMP redirect message to the remote system. in.ripngd starts automatically with the system boot time by creating /etc/inet/ndpd.conf file. In such case, transfer path information of IPv6 is deployed to the adjacent router. In order to avoid deploying the transfer path information, after configuring an ip parameter by the following procedure, start in.ripngd with –q option. Note, system reboot is not necessary to enable the following steps.

In the case of a Solaris 8 or Solaris 9:
/usr/sbin/ndd -set /dev/ip ip6_forwarding 1
/usr/sbin/ndd -set /dev/ip ip6_send_redirects 1
/usr/sbin/ndd -set /dev/ip ip6_ignore_redirect 1
/usr/lib/inet/in.ripngd -q

In the case of a Solaris 10:
/usr/sbin/routeadm -e ipv6-forwarding
/usr/sbin/routeadm -e ipv6-routing
/usr/sbin/routeadm -s ipv6-routing-daemon="/usr/lib/inet/in.ripngd"
/usr/sbin/routeadm -s ipv6-routing-daemon-args="-q"
/usr/sbin/routeadm -u

D.2.9 Incorrect operation by the user

D.2.9.1 Accidentally deleted the virtual interface with ifconfig command

Phenomenon:

Unable recover the virtual interface of a Fast switching mode deleted with ifconfig command by accident.

Cause and how to deal with:

There would be no guarantee on system behavior, if a virtual interface (Fast switching mode) is disabled or deleted. In order to recover a virtual interface, follow the procedure below:

[Example 1]

Accidentally executing “ifconfig sha0 unplumb” against a virtual interface sha0 for Fast switching mode.

If IPv4 address is being used: # ifconfig sha0 plumb *IPv4 address* up IPv6 address is being used: # ifconfig sha0 inet6 plumb # ifconfig sha0:2 inet6 plumb *IPv6 address* (Execute only if a logical virtual interface is configured) # ifconfig sha0 inet6 up # ifconfig sha0:2 inet6 up (Execute only if a logical virtual interface is configured)

[Example 2]

Accidentally executing “ifconfig sha0 down” against a virtual interface sha0 for Fast switching mode.

If IPv4 address is being used: # ifconfig sha0 up IPv6 address is being used: # ifconfig sha0 inet6 up # ifconfig sha0:2 inet6 up (Execute only if a logical virtual interface is configured)

In the case of a cluster system, a virtual interface is restored automatically. In addition, please refer to "2.3.4 Interface status monitoring feature" automatically about the virtual interface which can be restored.

D.2.10 System in Solaris zone

D.2.10.1 Patch application fails

Symptom:

When a patch is applied with the "patchadd" command after the system is rebooted in single user mode, the following error message is output then patch application fails.

```
Preparing checklist for local zone check...

Checking local zones...

Booting local zone zone0 for patch check...
  ERROR: unable to boot zone: problem running </usr/sbin/zoneadm> on zone
<zone0>: Error 0
could not verify net address=192.168.80.10 physical=sha0: No such device or address
zoneadm: zone zone0 failed to verify

Can not boot local zone zone0
```

Corrective action:

If a Solaris zone exists on the system, consistency with a non-global zone will be checked at the time of patch application. If the non-global zone is used in the high-reliability network through redundant line control, a consistency error will occur then patch application will fail. It is necessary to apply the patch using the following steps:

[Procedure]

1) Start the system in multi-user mode.

2) Check that the redundant line control function is activated.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
```

3) Change the mode from multi-user to single user mode using the "init" command.

```
# init s
```

4) Apply the patch.

```
# patchadd “<Patch-ID>”
```

Glossary

This appendix provides glossary as a tool for studying this users guide. This glossary includes terms that are frequently used when discussing the document. Users can find definitions of unfamiliar words, or of familiar words that may have an unfamiliar meaning in the context of this document.

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 commmunication alive during transfer route failure and increases the total throughput by multiplexing transfer routes between servers on the same network.

Global zone

A global zone is the global view of the Solaris operating environment. There is always one global zone per Solaris instance. Each software partition that is created within the Solaris instance can be managed and controlled in the global zone.
[Related article] Solaris zones, Non-global zone (Zone)

GS/SURE linkage mode

GS/SURE linkage mode multiplexes transfer routes between global server/SURE SYSTEM and ExINCA lies on the same network. This mode provides functionality of transfer route failover during transfer route failure in which implements high availability.

HUB-to-HUB monitoring function

A function to monitor an error in the connection between the HUBs (cascade connection). The monitoring range is from an active interface to a HUB connected to an active interface, and to the one connected to a standby interface. This function includes the monitoring range of a HUB monitoring function. However, it does not monitor a standby interface.
[Related article] HUB monitoring function

LAN card

The same meaning as that of NIC.

Line monitoring

The same meaning as that of HUB monitoring function.
[Related article] Inter-HUB monitoring function

Logical interface

A logical interface created in a different name to the same one physical interface. For instance, a logical interface to a physical interface eth0 is eth0:X (X is 0, 1, 2...)
[Related article] Logical IP address

Logical IP address (logical IP)

An IP address assigned to a logical interface.
[Related article] Logical interface

Logical IP address takeover function

A function to take over a logical IP address from cluster to cluster. It is possible to take over a logical IP address if switching from an active node to a standby node occurred between clusters. A physical IP address is not taken over in this case.

Logical virtual interface

Logical virtual interface is a logical interface created as distinguished name for a virtual interface. For example, a logical virtual interface for the virtual interface sha0 is represented as sha0:X (X

refers to 2,3..64).
Note that if X becomes larger than 65, they are then used as a takeover virtual interface on a cluster environment.

Monitoring frame

A Monitoring frame is an unique frame GLS handles to monitor the transfer paths. Fast switching mode uses this feature to monitor associate host. For NIC switching mode, it uses this feature as standby patrol function to monitor standby interfaces.
[Related article] Standby patrol function, HUB monitoring function, Inter-HUB monitoring function

NIC sharing function

A function to create more than one piece of configuration information by sharing the NIC if the adding physical IP address is the same in all NICs and configuration information. Use this function to assign more than one IP to a pair of the redundant NICs. Use this to execute cluster mutual standby operation as well.

NIC switching mode

A mode to realize high reliability by exclusively using a redundant NIC and switching when an error occurred. It is necessary to connect a redundant NIC in the same network in this mode.

Non-global zone (Zone)

Each non-global zone has a security boundary around it. The security boundary is maintained by allowing zones to only communicate between themselves using networking APIs.
[Related article] Solaris zones, Global zone

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.

RIP mode

Routing Information Protocol (RIP) mode multiplexes transfer routes connected between the servers on a remote network. This mode provides functionality of transfer route failover during transfer route failure in which implements high availability.

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".

Router/HUB monitoring function

A function to monitor from an active interface to a Router/HUB connected to an active interface. It

switches to a standby interface if detected an error.
[Related article] Inter-HUB monitoring function, Line monitoring

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

Solaris Containers

Solaris container isolate software applications and services using flexible, software-defined boundaries. This software partitioning enables administrators to easily create many private execution environments in a single instance of the Solaris Operating System. It also enables dynamic control of applications and resource priorities. For details, see the "Solaris 10 OS manual".

Standby interface

An interface currently not used for communication, but to be used after switched.
[Related article] Active interface

Standby patrol function

A function to monitor the status of a standby interface in NIC switching mode. Monitoring a standby interface regularly detects a failure of NIC switching in advance. Standby patrol is to send a monitoring frame from a standby interface to an active interface and monitor its response. The monitoring range is from a standby interface to a HUB connected to a standby interface, a HUB connected to an active interface, and an active interface. This includes the monitoring range of an inter-HUB monitoring function. Therefore, it is not necessary to use an inter-HUB monitoring function when using a standby patrol function. The monitoring range of inter-HUB monitoring is from an active interface to a HUB connected to an active interface and the one connected to a standby interface, without including a standby interface.
[Related article] Standby patrol function (automatic fail-back if a failure occurs), Standby patrol function (immediate automatic fail-back)

Standby patrol function (automatic fail-back if a failure occurs)

A standby patrol function to automatically incorporate the failed interface as a standby interface when it recovered. This function automatically incorporates the failed primary interface as a standby interface when it recovered. This makes it possible to fail back to a primary interface if an error occurred in a secondary interface.
[Related article] Standby patrol function, Standby patrol function (immediate automatic fail-back)

Standby patrol function (immediate automatic fail-back)

A standby patrol function to fail back immediately after the failed interface recovered. When the failed primary interface recovered, this function immediately fails it back as an active interface. A secondary interface is incorporated as a standby interface in this case.
[Related article] Standby patrol function, Standby patrol function (automatic fail-back if a failure occurs)

Tagged VLAN (IEEE802.1Q)

Tagged VLAN attaches an identifier called a "tag" to communication packets of each network allow to build multiple virtual networks on the same physical line.

Tagged VLAN interface

Tagged VLAN interface is a logical interface generated from a NIC that supports Tagged VLAN functionality (IEEE802.1Q).

Takeover virtual interface

Takeover virtual interface is an interface of GLS, which takes over an interface between the cluster nodes. Takeover virtual interface is configured with a logical virtual interface containing logical number of 65 or later.

User command execution function

This refers execution of a command manually operated by the user.
[Related article] NIC switching mode, GS/SURE linkage mode

Virtual 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

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".

Abbreviations

DR
: Dynamic Reconfiguration

GLS
: Stands for Global Link Services.

GS
: Global Server

LAN
: Local area network

NIC
: Stands for Network Interface Card. Also called a LAN card.

PHP
: PCI Hot Plug

SIS
: Stands for Scalable Internet Services.

RIP
: Routing Information Protocol

RMS
: Reliant Monitor Services.

VLAN
: Virtual LAN

Index