PRIMECLUSTER Global Link Services Configuration and Administration Guide:

Redundant Line Control Function V4.1

Preface

This manual describes PRIMECLUSTER GLS (Redundant Line Control Function) and explains the installation and operation management procedures. GLS is the abbreviated name for Global Link Services.

Intended Reader

This manual is intended for the system manager who manages the implementation and operation of PRIMECLUSTER Global Link Services (Redundant Line Control Function).

The manager is assumed to have an understanding of PRIMECLUSTER, which is the fundamental program for cluster control. Read the description of "cluster service" or "service" as "Cluster Application (userApplication)".

Organization of This Manual

This manual is organized as follows:

Chapter 1 Outline

This chapter provides an outline of Redundant Line Control Function.

Chapter 2 Functions

This chapter explains the line duplicating function provided by Redundant Line Control Function.

Chapter 3 Installation

This chapter explains how to operate setting up Redundant Line Control Function.

Chapter 4 Operation

This chapter explains how to operate Redundant Line Control Function.

Chapter 5 Operation on Cluster System

This chapter explains how to operate Redundant Line Control Function on cluster system.

Chapter 6 Maintenance

This chapter describes the data required for a Redundant Line Control Function troubleshooting.

Chapter 7 Command References

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

Appendix A Message List

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

Appendix B Examples of Setting Up

This appendix describes examples of Redundant Line Control Function setting up.

Appendix C Changes from old versions

This appendix describes the changes from old versions.

Appendix D Others

This appendix describes the supplement matters.

Trademarks

UNIX is a trademark of X/Open Company limited and licensed exclusively by the company in the U.S.A. and other countries.

Solaris is a registered trademark of Sun Microsystems:, Inc. of the United States.

Ethernet is a registered trademark of Fuji Xerox Co.:, Ltd.

August 2002

First edition: August 2002

Announce:

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 power reactioncore control in nuclearatomic facility, airplane automatic aircraft flight control, air traffic control, operation control in mass transport control systems, medical instrument for life support system, missile launching control in weapon system. You shall not use this Product without securing the sufficient safety required for such High Safety Required Use. If you wish to use this product for High Safety Required Use, please consult with a senior sales representative of the company supplying this product, before such use.

Notes:

The contents of this document shall not be reproduced in any from without the prior permission of Fujitsu Limited.
This document is subject to change without prior notice.

Chapter 1 Outline

1.1 What is Redundant Line Control Function?

Redundant Line Control Function is a software program that makes the network line of a local system redundant with several Network Interface Cards (NICs) to realize high-reliability communications.

Redundant Line Control Function provides line control functions in the following four modes.

Fast switching mode

Fast switching mode enables the system to control lines by a unique method. In this method, multiplexed lines are used concurrently. In the event of a fault, the system cuts off the faulty line and operates on a reduced scale. The unique method allows early fault detection but is limited to remote systems using the same model. This mode cannot be used to communicate with a host on other networks connected via routers.

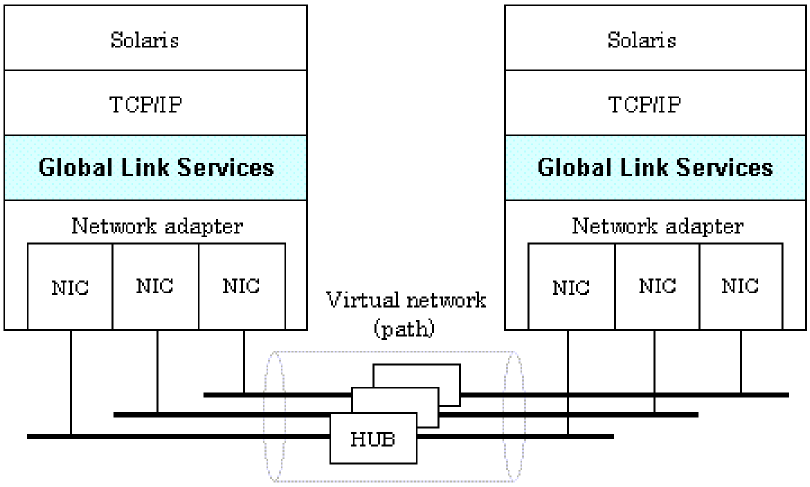


Figure 1.1 Fast switching mode

RIP mode

RIP mode enables the system to control lines by a standard protocol called Routing Information Protocol (RIP). In this mode, either of the duplicated paths is used according to RIP information. In the event of a fault, the system switches to the other path. The standard protocol allows communications with non-limited parties and also with host systems on other networks connected via routers. However, paths switching in the RIP mode is slow and time-consuming.

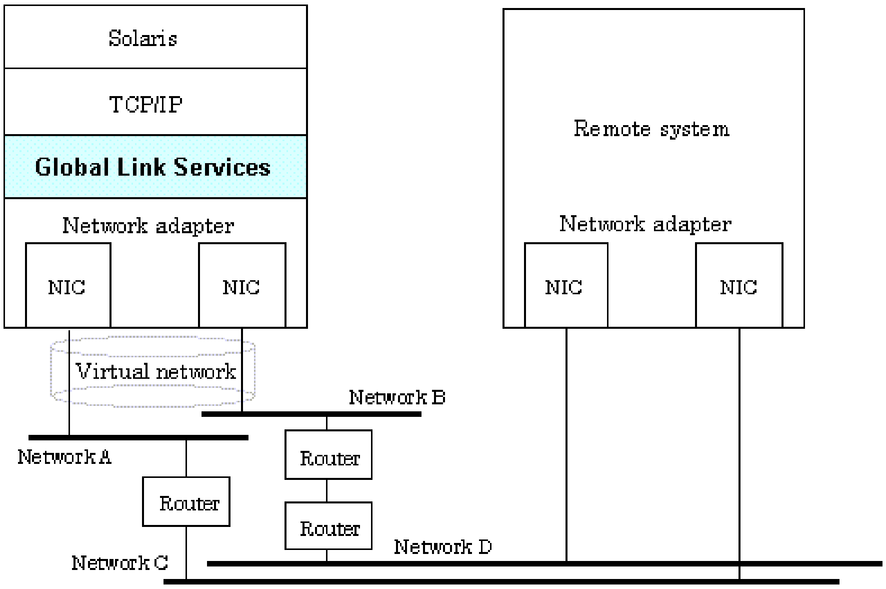


Figure 1.2 RIP mode

NIC switching mode

NIC switching mode enables the system to control line switching by connecting redundant NICs (LAN cards) in the same network and using one of them exclusively. In this mode, communications are not limited to specific remote systems. Communications with host systems on other networks via routers is also allowed.

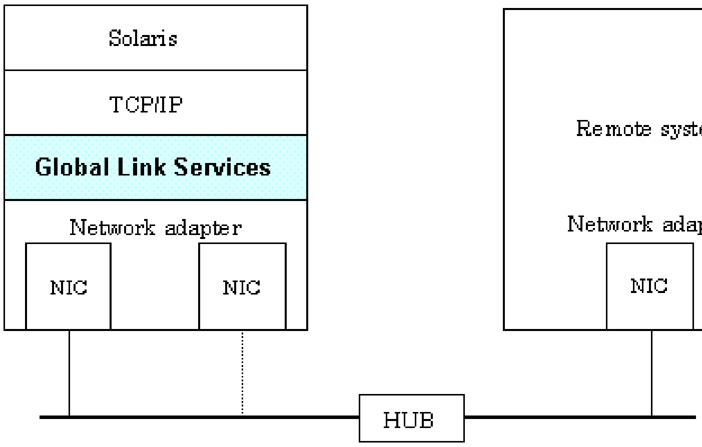


Figure 1.3 NIC switching mode

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.

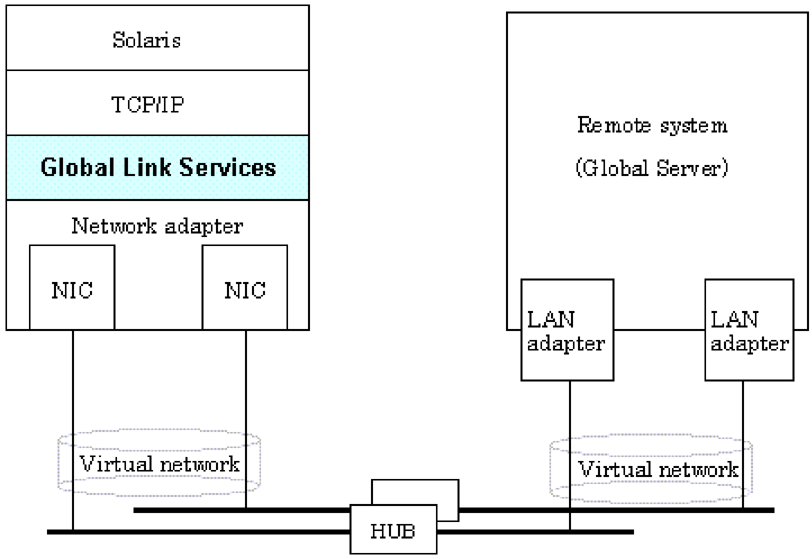


Figure 1.4 GS/SURE linkage mode (GS/SURE communication function)

TCP relay function

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

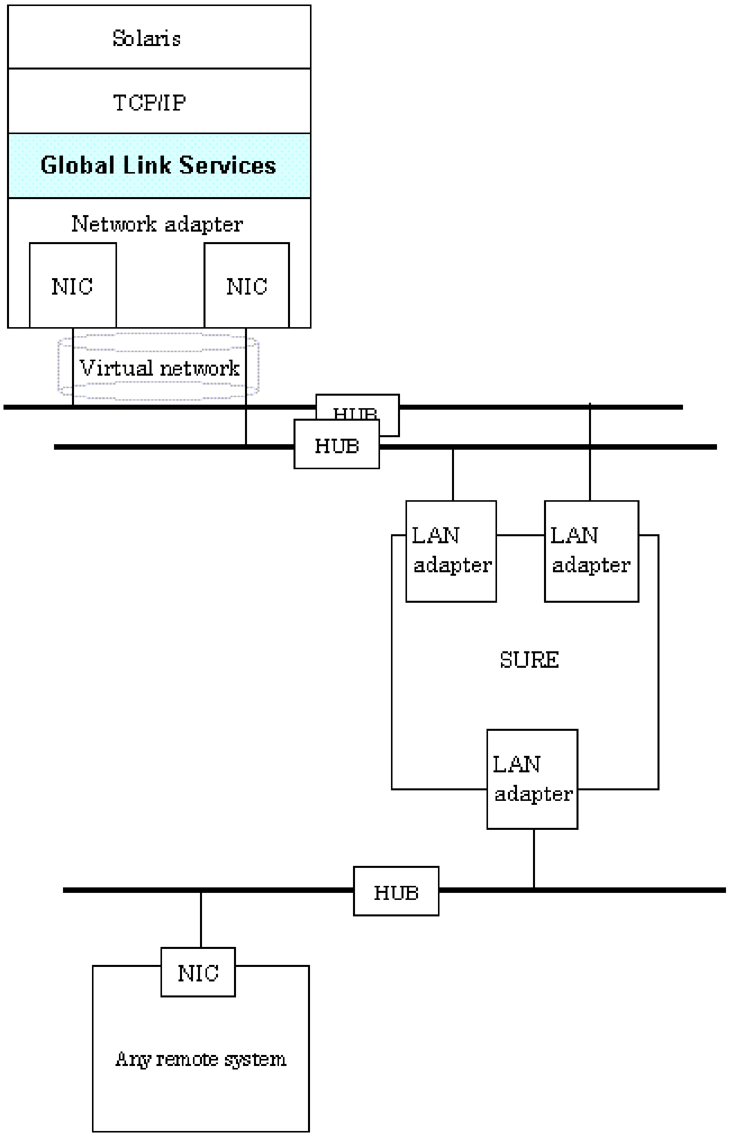


Figure 1.5 GS/SURE linkage mode (TCP relay function)

Functional comparison

Table 1.1 compares the functions of various modes:

Table 1.1 Functional comparison table (continued)

Mode		Fast switching mode	RIP mode
Fault monitoring function	Fault monitoring	Monitoring by sending/receiving unique frames. If a line failure is detected, the system disconnects the faulty line to operate on a reduced scale.	Monitoring by sending/receiving RIP packets. If a faulty line is detected, the system switches to the other line. If the router monitoring function (optional) is used, the ping command is used for router monitoring. If a faulty line is detected, the system switches to the other line.
	Switching time	About 10 seconds	If the router monitoring function is not used: about 5 minutes If the router monitoring function is not used: about 1 to 5 minutes (depending on the setting and operating conditions)

	Detectable failures	NIC failure, cable failure, and HUB failure	NIC failure, cable failure, HUB failure, and router failure
	Fault monitoring start/stop	The fault monitoring is started automatically when the Virtual interface is activated and is automatically stopped when the Virtual interface is inactivated.	The same as the left
Switching function	Switching operation	NIC that cannot communicate is automatically disconnected. The faulty NIC can also be disconnected manually with an operational command.	The path is switched in accordance with the RIP routing information.
	Failback operation	The faulty NIC is monitored for recovery. When the NIC becomes capable of communication, the failback operation is automatically performed so that it can be reused for communication. The failback operation can also be performed manually with an operational command.	The failback of path is performed in accordance with the RIP routing information.
NIC sharing function (*1)		In Fast switching mode, RIP mode, and Fast switching/RIP mode, all or some of the NICs can be shared.	The same as the left
Connectable remote device		PRIMEPOWER,GP7000F	Any device. Fujitsu recommends using the Fujitsu LINLRELAY Series as the router to be connected on the local system.

*1 The NIC sharing function is a function with which the system operates in multiple line control mode using a pair of redundant NICs (this setup is stored in the so-called configuration information).

Table 1.1 Functional comparison table (end)

Mode		NIC switching mode	GS/SURE linkage mode
Fault monitoring function	Fault monitoring	Monitoring of HUB by using the ping command. If a faulty line is detected, the system switches to the standby NIC.	Monitoring of the LAN adapter of the device with which communication is to be carried out by using the ping command. If a faulty line is detected, the system switches to the other path.
	Switching time	About 10 seconds to 3 minutes (depending on the setting)	The same as the left
	Detectable failures	NIC failure, cable failure, and HUB failure	The same as the left
	Fault monitoring start/stop	The fault monitoring is started automatically when the Virtual interface (logical IP) is activated and is automatically stopped when the Virtual interface is inactivated. It is also possible to start/stop fault monitoring manually with an operational command.	The fault monitoring is started automatically when the Virtual interface is activated and is automatically stopped when the Virtual interface is inactivated. It is also possible to start/stop fault monitoring manually with an operational command.
Switching function	Switching operation	The currently operating Physical interface is made automatically to go down and then the standby Physical interface is made to go up. It is also possible to switch the Physical interface manually with an operational command.	NIC that cannot communicate is automatically disconnected. The faulty NIC cannot be disconnected manually.
	Failback operation	The failback of an NIC can be performed manually with an operational command. The failback of an NIC is also performed automatically with the standby patrol function.	The faulty NIC is monitored for recovery. When the NIC becomes capable of communication, the failback operation is automatically performed so that it can be reused for communication. The failback operation cannot be performed manually.

NIC sharing function	Not possible to share any NIC used in NIC switching mode with the other modes. However, possible to define more than one virtual interface and share NIC only when using all NICs in one piece of the configuration information under the same conditions in NIC switching mode.	Not allowed
Connectable remote device	Any device	GS/SURE (if the GS/SURE communication function is used) or any device (if the TCP relay function is used)

Which of the four modes to use depends on the operating conditions of each system. Figure 1.6 shows the criteria for selecting the mode.

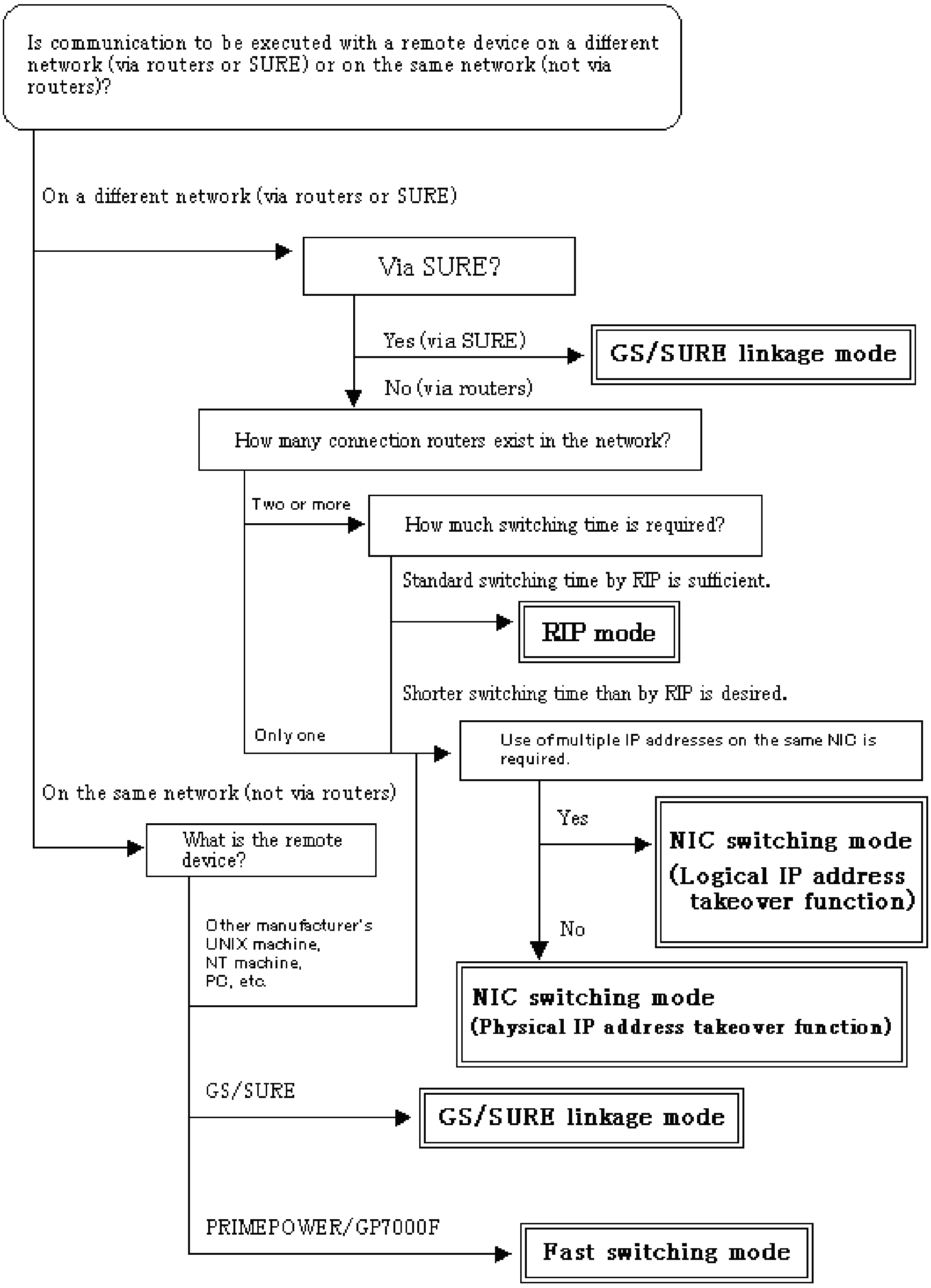

Is communication to be executed with a remote device on a different network (via routers or SURE) or on the same network (not via routers)?
On a different network (via routers or SURE)
Via SURE?
Yes (via SURE)
GS/SURE linkage mode
No (via routers)
How many connection routers exist in the network?
Two or more
How much switching time is required?
Standard switching time by RIP is sufficient.
RIP mode
Shorter switching time than by RIP is desired.
Only one
Use of multiple IP addresses on the same NIC is required.
Yes
NIC switching mode (Logical IP address takeover function)
No
NIC switching mode (Physical IP address takeover function)
On the same network (not via routers)
What is the remote device?
Other manufacturer's UNIX machine, NT machine, PC, etc.
GS/SURE
GS/SURE linkage mode
PRIMEPOWER/GP7000F
Fast switching mode

Figure 1.6 Criteria for deciding on a duplication mode

1.2 Benefits of Redundant Line Control Function

Redundant Line Control Function can construct high-reliability network with exellent fault resistance and availability.

1.3 System Configuration

Fast switching mode and RIP mode

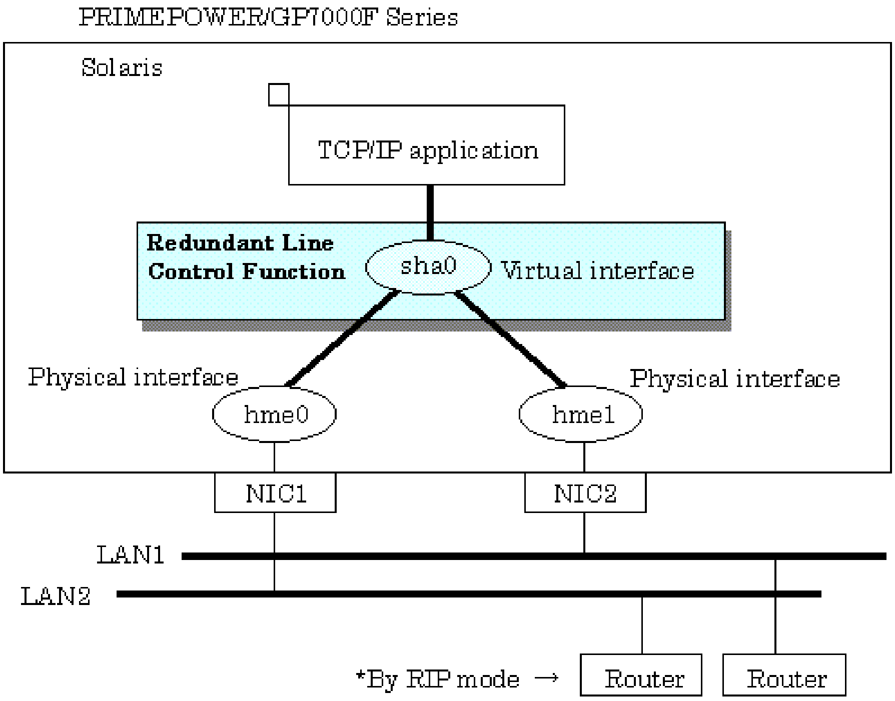


Figure 1.7 Fast switching mode and RIP mode

NIC switching mode

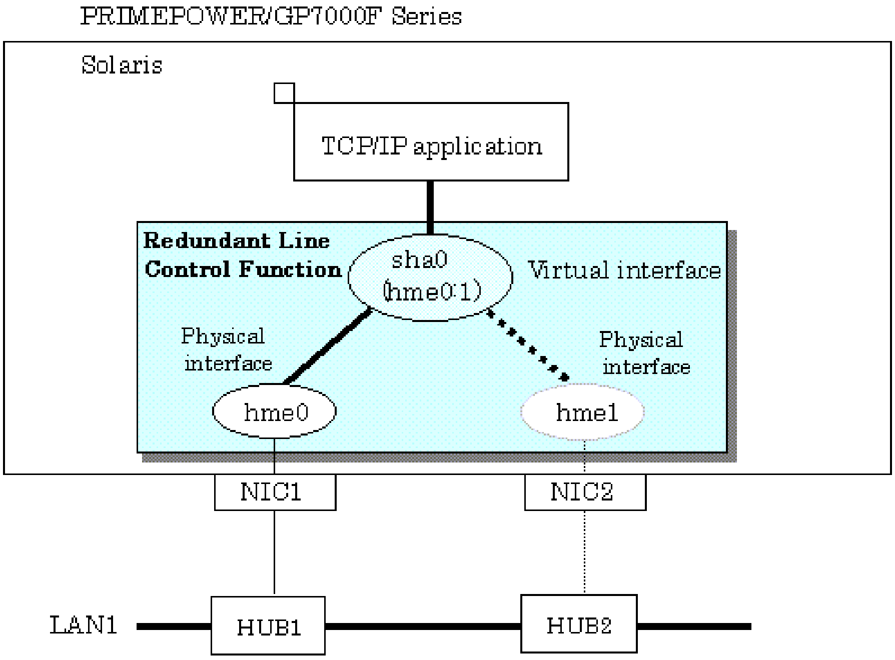


Figure 1.8 NIC switching mode

GS/SURE linkage mode

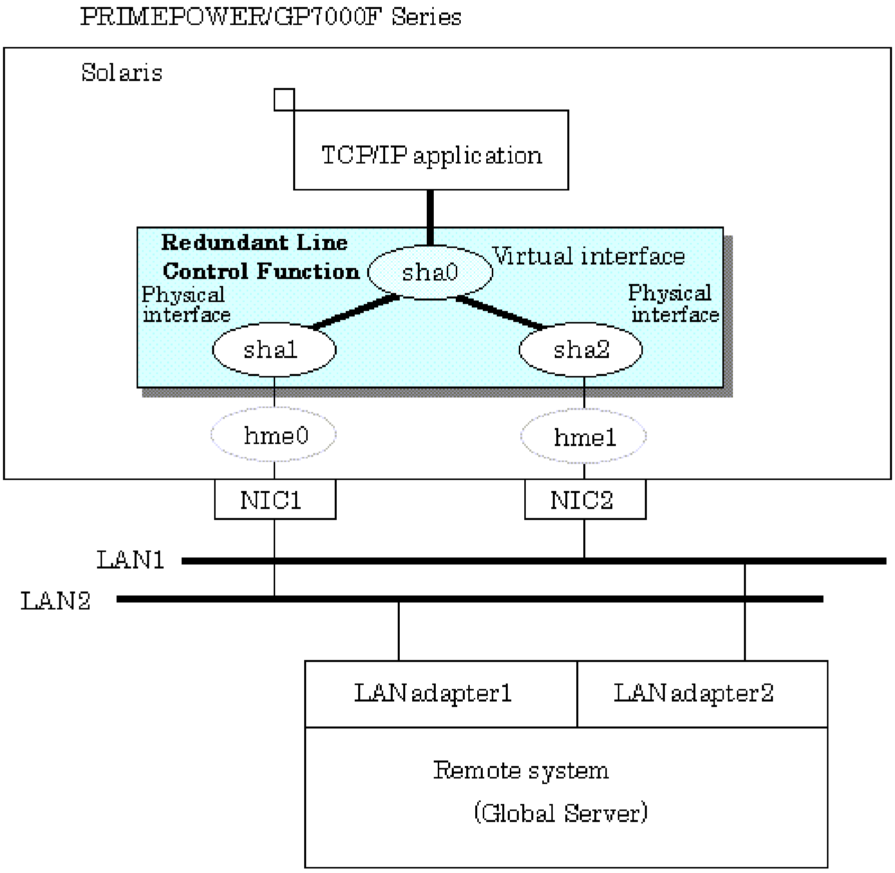


Figure 1.9 GS/SURE linkage mode (GS/SURE communication function)

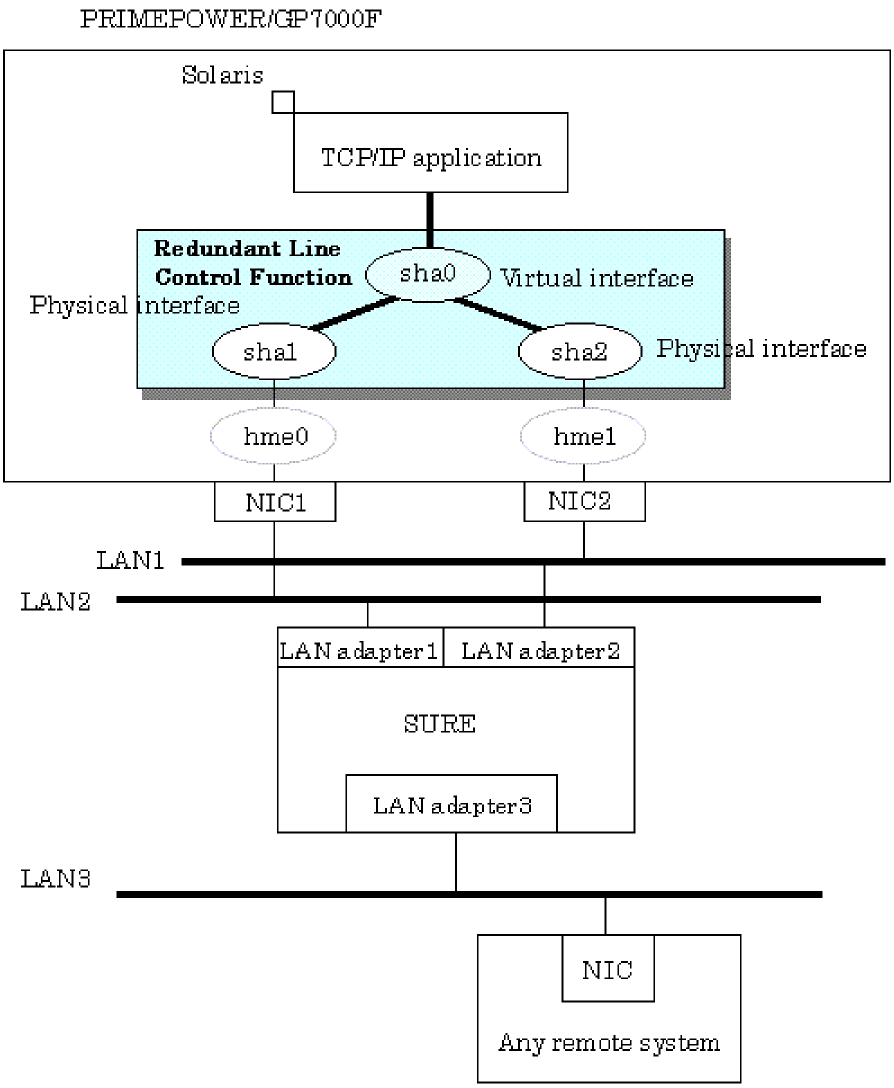


Figure 1.10 GS/SURE linkage mode (TCP relay function)

Redundant Line Control Function consists of the following components:

Main unit

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

Router (for operation in RIP mode)

The use of the following router is recommended:

Fujitsu LINKRELAY Series

HUB (for operation in NIC switching mode)

The following HUB can be used:

HUB to which IP address can be set

Operating system (OS)

Solaris 8 (32-bit and 64-bit modes)

Interfaces

Redundant Line Control Function uses the following interface:

Physical interface

The Physical interface is an interface generated by each NIC. The interface name is determined by checking the NIC type (such as hmeX and qfeX). In GS/SURE linkage mode, however, the interface name is shaX because Redundant Line Control Function constitutes a Physical interface.

Virtual interface

The Virtual interface is an interface (such as sha0 and sha1) generated by Redundant Line Control Function. TCP/IP applications using Redundant Line Control Function conduct communications via a virtual network (virtual IP address) allocated to this interface. Even though the Virtual interface name is used as an identifier of the configuration information, in NIC switching mode, no virtual network is generated. In this case, a logical IP address is allocated to a real network. TCP/IP applications using Redundant Line Control Function conduct communications via this logical IP address.

In a Redundant Line Control Function, necessary to assign a network number and an IP address in each method as follows:

Network number

Fast switching mode, RIP mode, and GS/SURE linkage mode

To assign a different network number to each physical interface, and a virtual interface.
For instance, necessary to assign three different network numbers in "Figure 1.7" because there are three interfaces in all.

NIC switching mode

To assign only one network number because a virtual network is not created in this mode.

IP address

Fast switching mode, RIP mode, and GS/SURE linkage mode

Necessary to assign one IP address to each physical interface, and a virtual interface. Possible to assign more than one IP address to a virtual interface by the setting. An address form possible to use is an IPv4 address. Not possible to use an IPv6 address.

NIC switching mode

Necessary to assign one IP address. Possible to assign more than one IP address by the setting. In NIC switching mode, it is possible to use both IPv4 and IPv6 addresses as an address form.

See "Chapter 2 The Functions" for the detail.

Chapter 2 Functions

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 packet that is to be sent is sent to an appropriate line based on the line conditions (whether any failure condition 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.

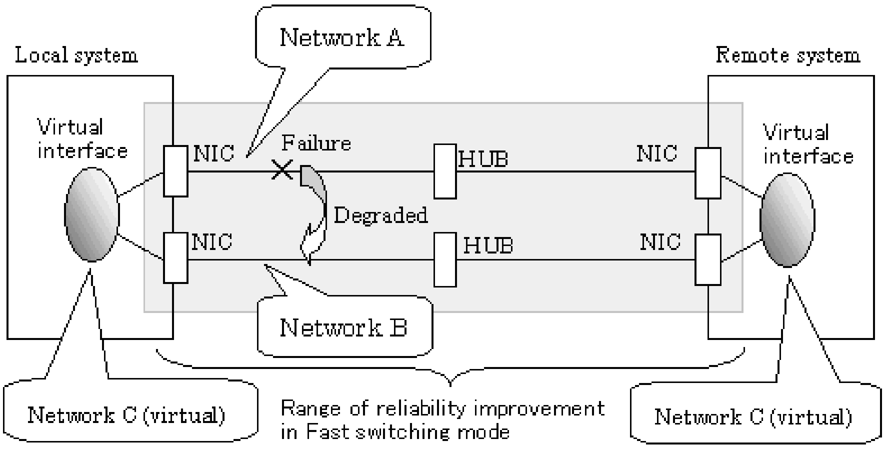


Figure 2.1 Example of duplicated operation in Fast switching mode

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:

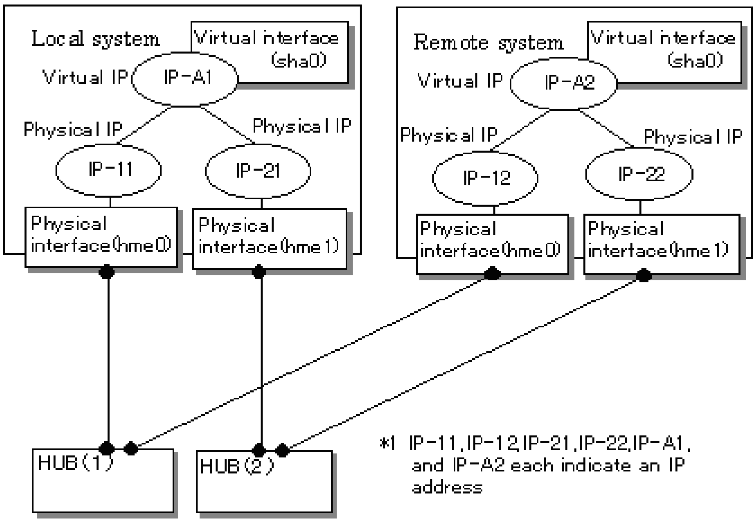


Figure 2.2 System configuration for Fast switching mode

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. An address form possible to specify is an IPv4 address. Not possible to specify an 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 local IP address to be allocated to the virtual interface for communication with remote devices. An address form possible to specify is an IPv4 address. Not possible to specify an 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. 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.

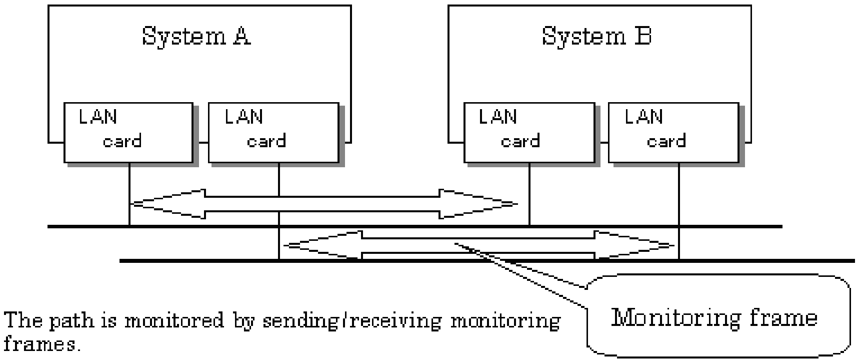


Figure 2.3 Monitoring method in Fast switching mode

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:

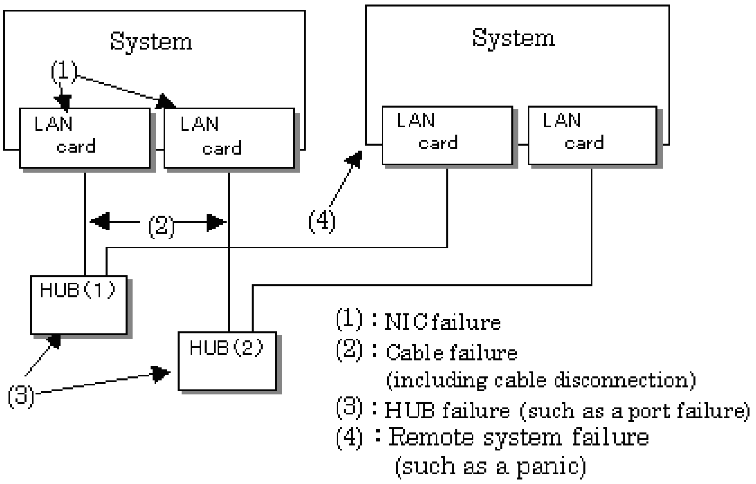


Figure 2.4 Detectable failures in Fast switching mode

Because the failures 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, 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 only lines operating normally are used to continue communication. Therefore, if at least one normal line remains, communication can continue without system reactivation. It is also possible to disconnect a specific line manually by using the operational command (hanetnic command).

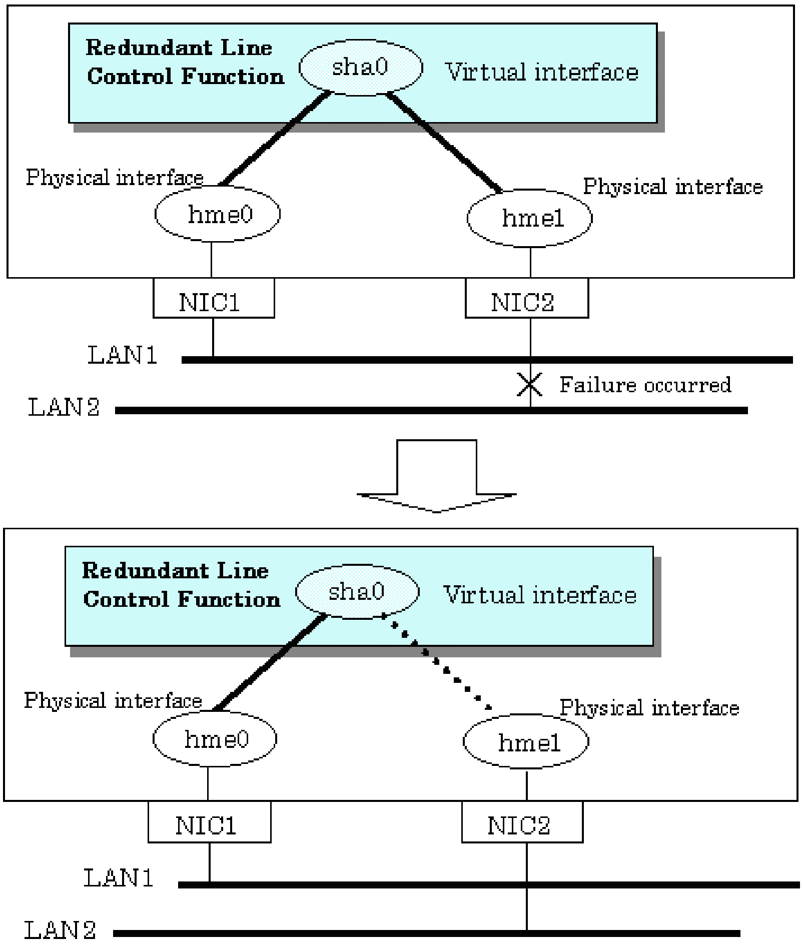


Figure 2.5 Outline of switching operation performed when a failure occurs in Fast switching mode

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 NIC sharing function

All or some of the NICs are shared among configuration information for which Fast switching mode, RIP mode, or Fast switching/RIP mode is set. (Not possible to share NICs that the other modes use.)

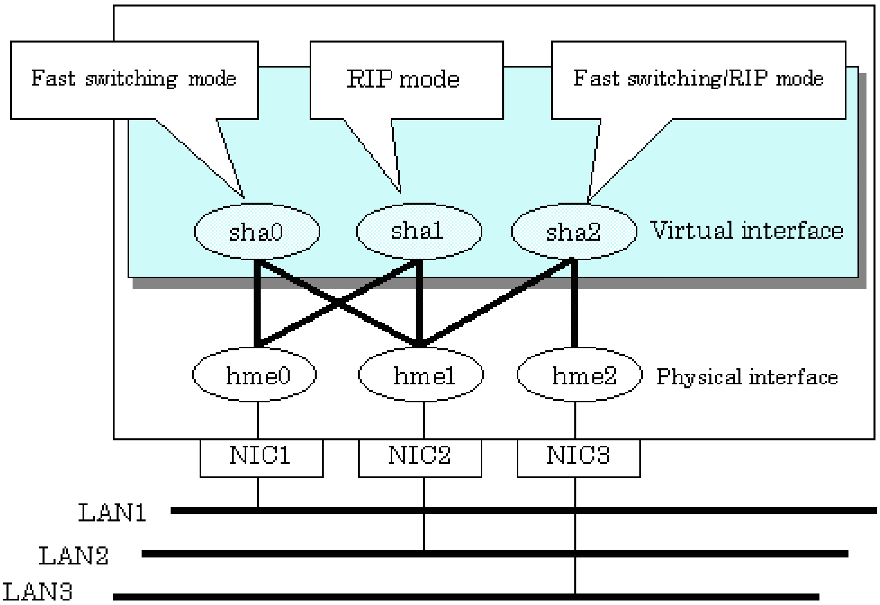


Figure 2.6 Example of the NIC sharing function

2.1.1.4 Connectable remote device

- PRIMEPOWER
- GP7000F

2.1.1.5 Available application

TCP/IP application using the TCP or UDP protocol

2.1.1.6 Notes

- No multi-cast IP address can be used.
- See "2.1.2.6 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.

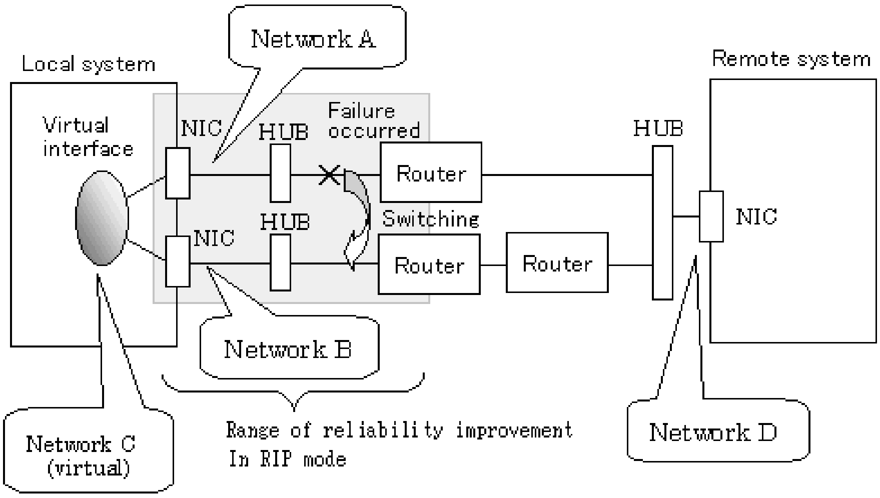


Figure 2.7 Example of duplicated operation in RIP mode

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 2.8 shows a system configuration for RIP mode:

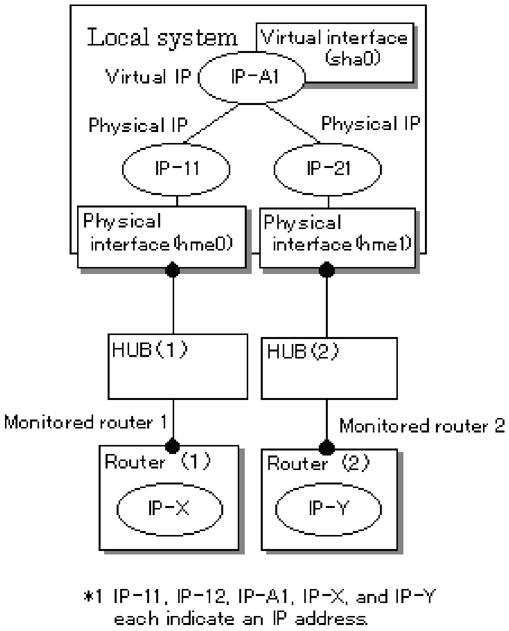


Figure 2.8 System configuration for RIP mode

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. An address form possible to specify is an IPv4 address. Not possible to specify an IPv6 address.

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. An address form possible to specify is an IPv4 address. Not possible to specify an IPv6 address.

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.

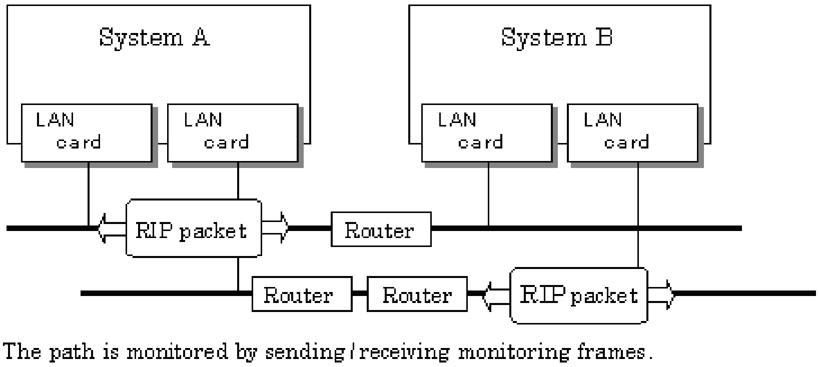


Figure 2.9 Monitoring method in RIP mode (when the router monitoring function is not used)

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:

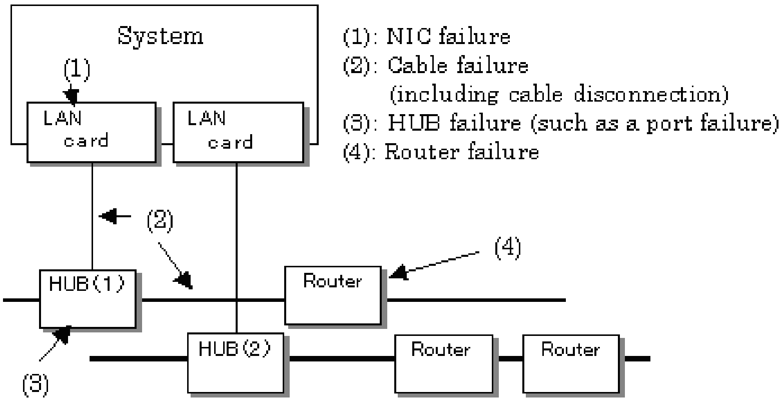


Figure 2.10 Effective monitoring range in RIP mode

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 service.

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.

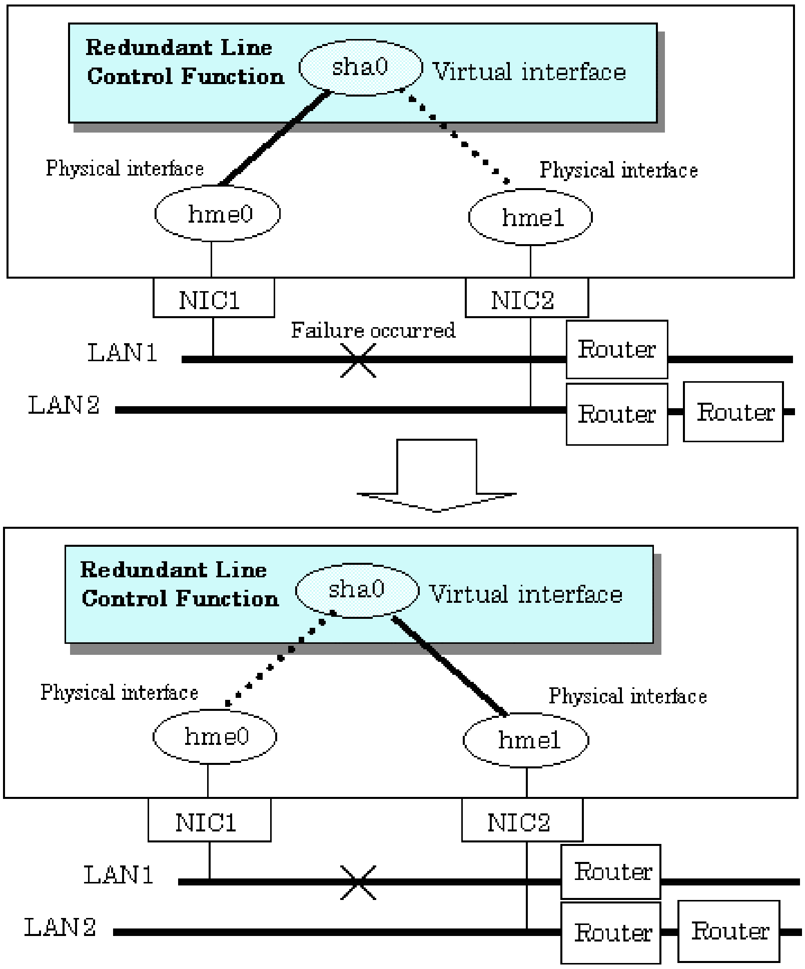


Figure 2.11 Outline of switching operation performed when a failure occurs in RIP mode

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 NIC sharing function

All or some of the NICs are shared among configuration information for which Fast switching mode, RIP mode, or Fast switching/RIP mode is set.

2.1.2.4 Connectable remote device

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

2.1.2.5 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).

2.1.2.6 Notes

- 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.

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.

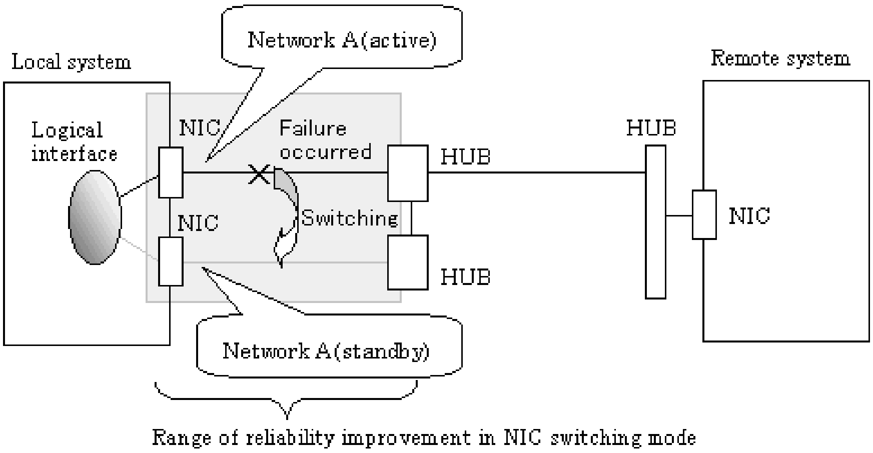


Figure 2.12 Example of duplicated operation in NIC switching mode

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 2.13 shows a system configuration for NIC switching mode:

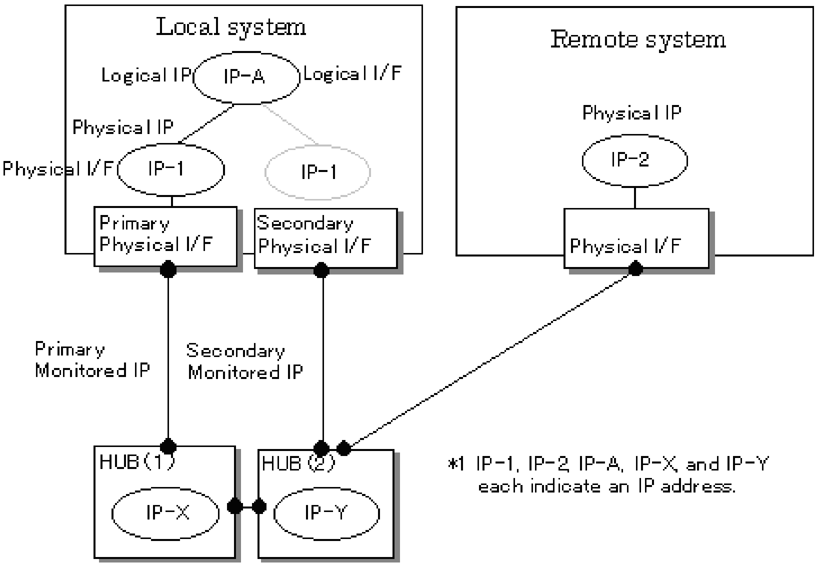


Figure 2.13 System configuration in NIC switching mode

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. An address form possible to specify is an IPv4 address. A link local address is automatically set as a physical IP for IPv6.

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. When using a physical IP address takeover function, it is not activated. In NIC switching mode, it is possible to use both IPv4 and IPv6 addresses as an address form.

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-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.

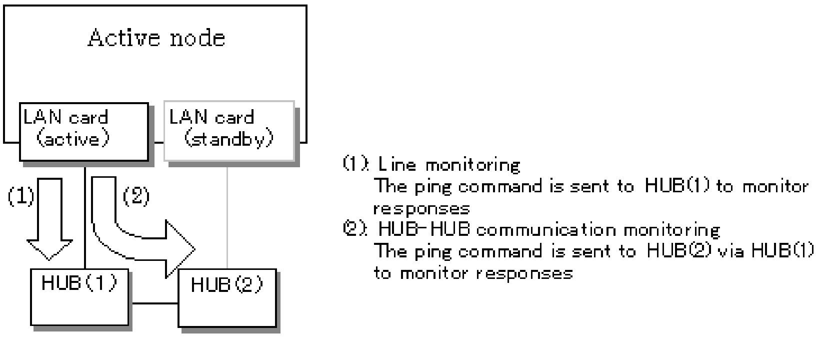

Active node
LAN card (active)
LAN card (standby)
(1)
(2)
HUB(1)
HUB(2)
(1): Line monitoring
The ping command is sent to HUB(1) to monitor responses
(2): HUB-HUB communication monitoring
The ping command is sent to HUB(2) via HUB(1) to monitor responses

Figure 2.14 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-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 an error occurred in a transfer route until [the time (sec) to wait for linkup] passed to wait for the Ethernet link to be established. Possible to set the time to wait 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.

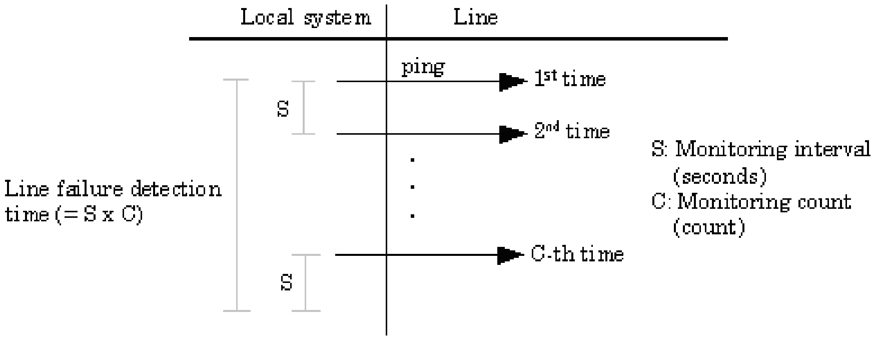

Local system
Line
ping
1st time
2nd time
C-th time
S
S
Line failure detection time (= S x C)
S: Monitoring interval (seconds)
C: Monitoring count (count)

Figure 2.15 Fault detection time in NIC switching time

Detectable failures

The following failures can be detected:

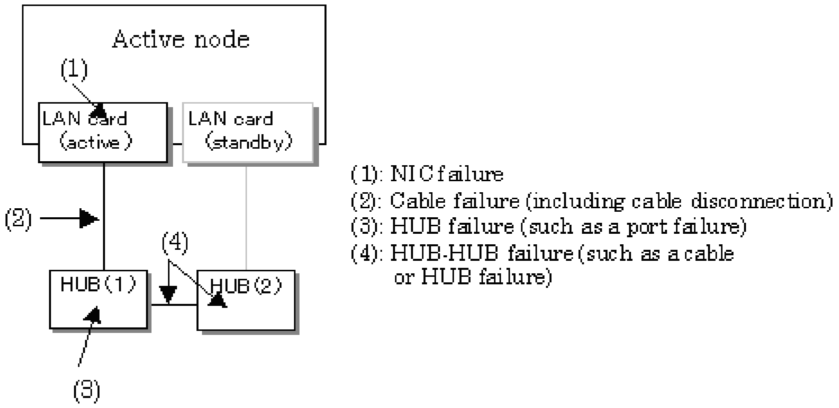

Active node
(1)
LAN card (active)
LAN card (standby)
(2)
(4)
HUB(1)
HUB(2)
(3)
(1): NIC failure
(2): Cable failure (including cable disconnection)
(3): HUB failure (such as a port failure)
(4): HUB-HUB failure (such as a cable or HUB failure)

Figure 2.16 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

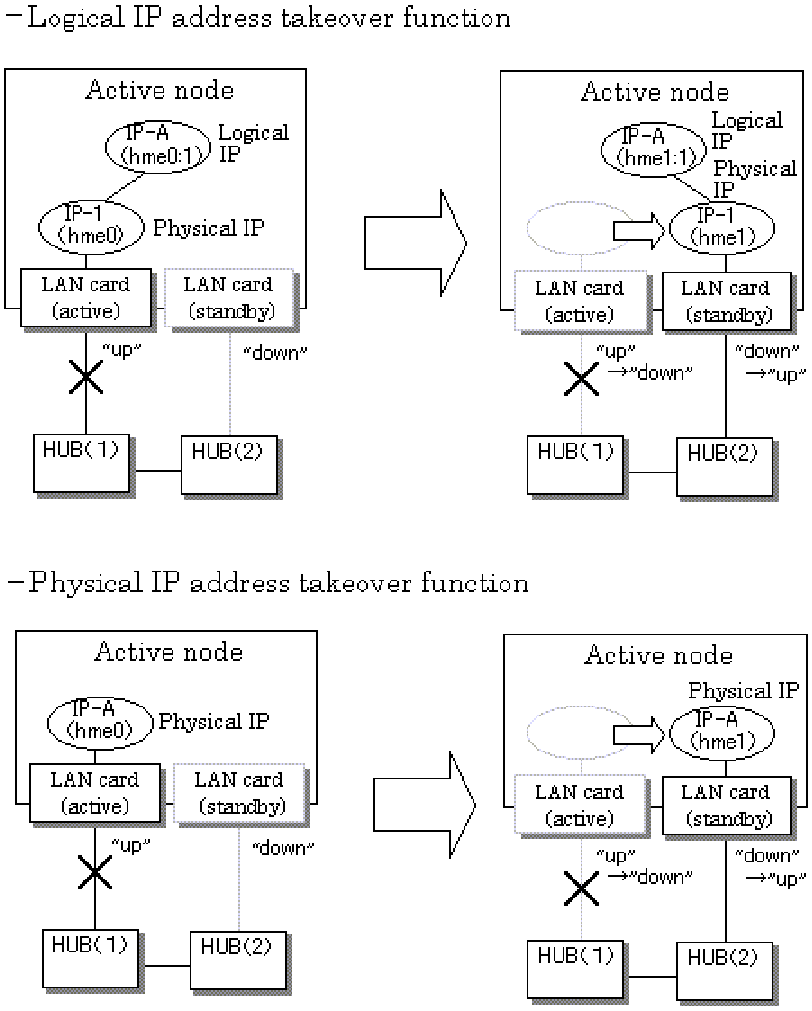
The line monitoring in NIC switching mode is automatically started when the system is activated and is automatically stopped when the system is stopped. In cluster operation, the line monitoring of each node is started and stopped independently. It is also possible to start or stop the line monitoring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

2.1.3.2 Switching function

Switching operation

The faulty NIC that is currently operating is made to go "down" and then the standby NIC is made to go "up" to operate as the new operating NIC. 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.
When using an IPv6 address, it is not possible to use a physical IP address takeover function.
Figure 2.17 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-HUB communication monitoring is enabled, a console message is output to the syslog file (/var/adm/messages).



－Logical IP address takeover function

－Physical IP address takeover function

Figure 2.17 Outline of switching operation performed when a failure occurs in NIC switching mode

Failback operation

The failback operation can be performed by using the hanetnic change command. The currently operating NIC is switched to the standby NIC and the standby NIC is switched to the operating NIC with this command (For details, see Chapter 7, Command References).

2.1.3.3 NIC sharing function

An NIC can be shared among configuration information for NIC switching mode only if all NICs and physical IP addresses added in configuration information are the same. Some of the NICs, though in the same operation mode, or NICs set in a different mode cannot be shared.

2.1.3.4 Connectable remote device

Any system can be connected.

2.1.3.5 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. (Remote party applications do not check the IP address.)

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. Packets to be sent 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.

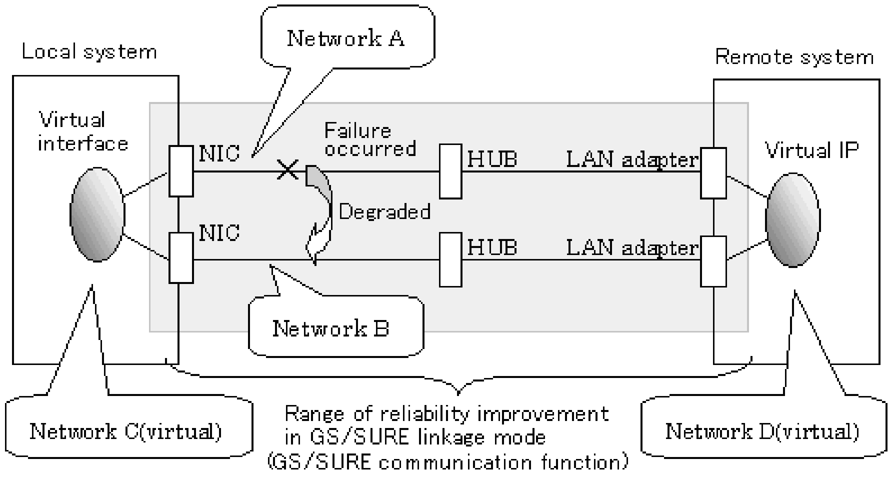


Figure 2.18 Example of duplicated operation in GS/SURE linkage mode (GS/SURE communication function)

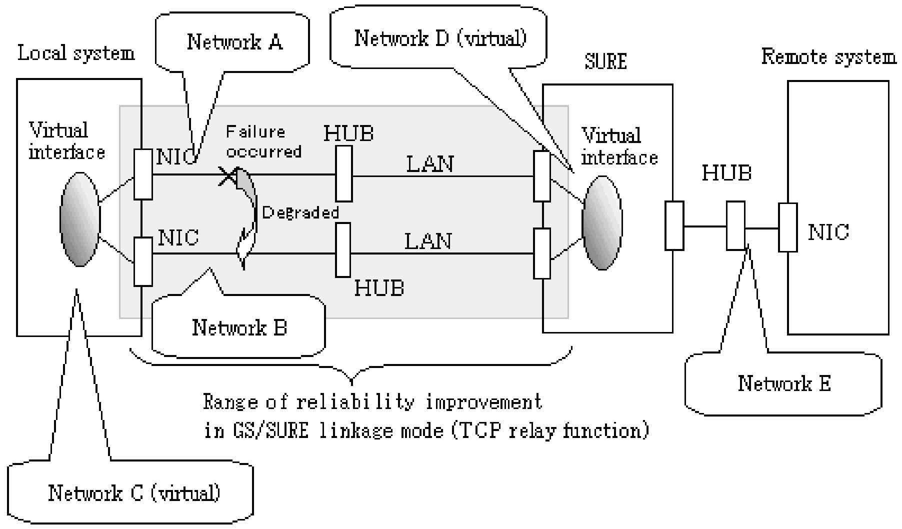


Figure 2.19 Example of duplicated operation in GS/SURE linkage mode (TCP relay function)

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

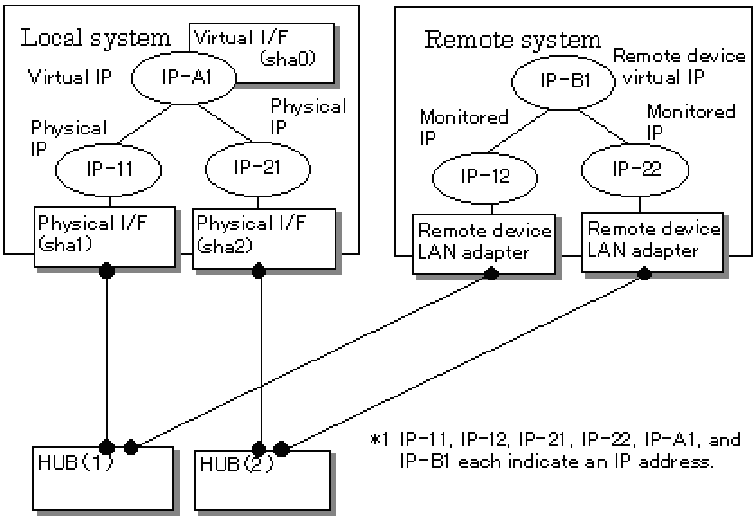
Lines are used in units of TCP connections for communication. If a failure occurs on a line, processing can continue on another line that is normal. Since all the redundant lines are activated for use, each of the lines can be directly used for a different purpose, enabling efficient use of resources.

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.

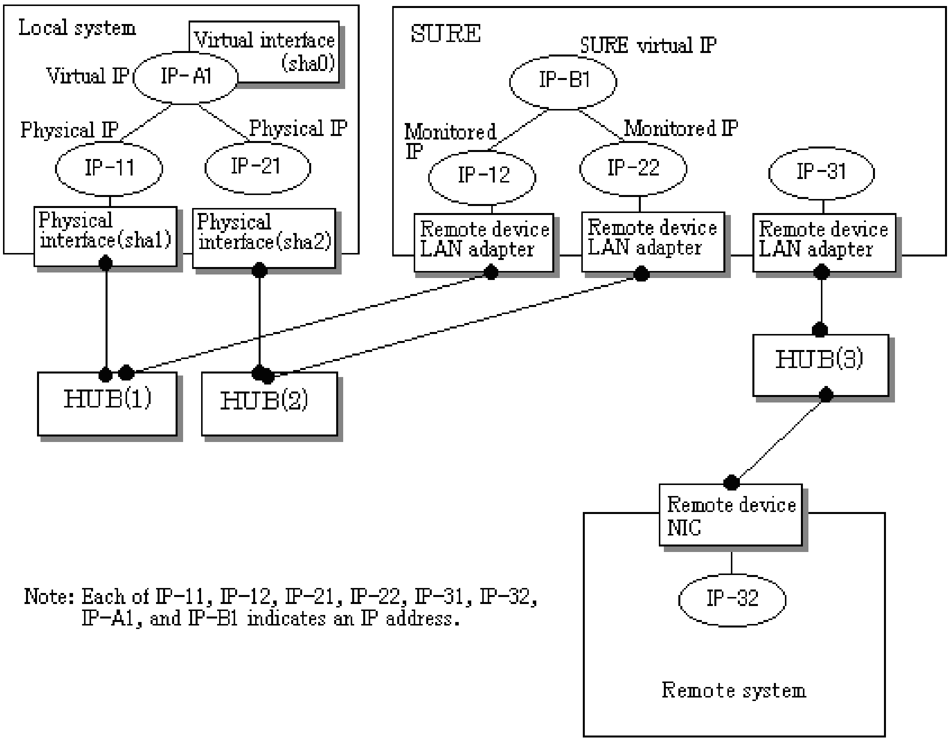
System configuration

Figures 2.20 and 2.21 show a system configuration of GS/SURE linkage mode (GS/SURE communication function) and of GS/SURE linkage mode (TCP relay function), respectively.



*1 IP-11, IP-12, IP-21, IP-22, IP-A1, and IP-B1 each indicate an IP address.

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



Note: Each of IP-11, IP-12, IP-21, IP-22, IP-31, IP-32, IP-A1, and IP-B1 indicates an IP address.

Figure 2.21 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 management view, etc. An address form possible to specify is an IPv4 address. Not possible to specify an IPv6 address.

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. An address form possible to specify is an IPv4 address. Not possible to specify an IPv6 address.

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. An address form possible to specify is an IPv4 address. Not possible to specify an IPv6 address.

Remote device virtual IP

Indicates a virtual IP of the remote device with which communication should be carried out. An address form possible to specify is an IPv4 address. Not possible to specify an IPv6 address.

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.

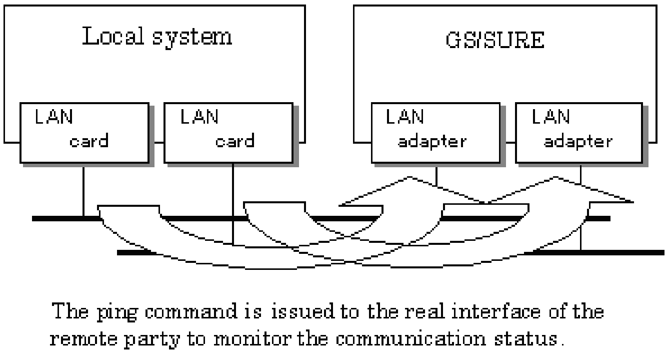

Local system
GS/SURE
LAN card
LAN card
LAN adapter
LAN adapter
The ping command is issued to the real interface of the remote party to monitor the communication status.

Figure 2.22 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. Set the switching time of a line up to 300 seconds in consideration of the switching time required when RIP is operating.

Detectable failures

The following failures can be detected:

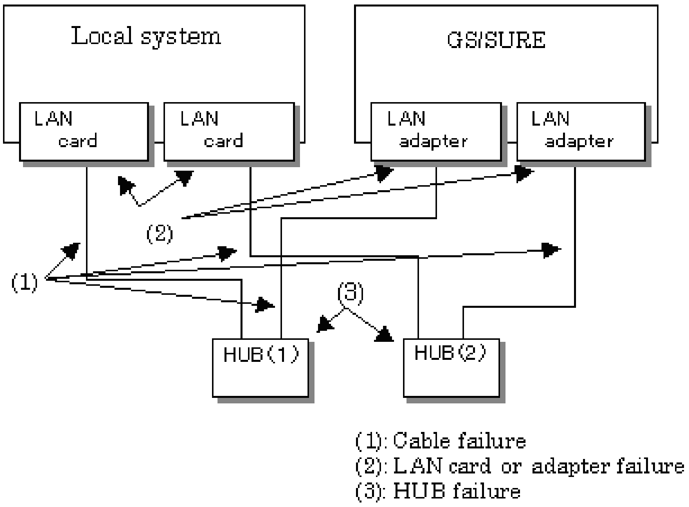


Figure 2.23 Detectable failures in GS/SURE linkage mode

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 NIC sharing function

The NIC sharing function cannot be used in this mode.

2.1.4.4 Connectable remote device

When using a GS/SURE communication function:

GS/SURE

When using a TCP relay function:

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

2.1.4.5 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.

2.1.4.6 Notes

When GS/SURE linkage mode is used, the system needs to be set as a multi-home host (in this case, an empty file called /etc/notrouter is created) instead of a router.

In this case, RIP mode or Fast switching/RIP mode cannot coexist. This mode cannot be used for communication between GPs.

2.2 Option Functions

The following option functions can be used in each mode.

Function	Mode			
	Fast switching mode	RIP mode	NIC switching mode	GS/SURE linkage mode
Multiple virtual interface definition function	A	A	A	A
Cluster failover function because of a line failure	A	X	A	X
Concurrent operation function with other modes via one virtual interface	A (*1)	A (*1)	X	X
Sharing function of physical interface	A (*2)	A (*2)	A (*3)	X
Multiple logical virtual interface definition function	A	A	O	X
Single physical interface definition function	A	A	A	A
Message output function when a line failure occurs	A	A (*4)	A	A
Router/HUB monitoring function	O	A (*4)	S (*5)	O
Communication party monitoring function	A (*6)	O	O	S (*7)
Standby patrol function	O	O	A	O
Dynamic adding/deleting/switching function of interfaces used	A (*8)	A (*8)	A (*9)	A (*8)
Automatic failback function	O	O	A	O
User command execution function	X	X	A	A
DR function	A	A	A	A

Explanation of symbols) S: Indispensable to set, A: Allowed, O: Replaced by other functions, X: Not allowed
*1: Concurrent operation between Fast switching mode and RIP mode is allowed.
*2: All or some of the NICs can be shared between Fast switching mode and RIP mode, but cannot be shared with other modes.
*3: Physical interfaces can be shared if all NICs and specified physical IP addresses are the same in the NIC switching mode.
*4: This function can be used by setting the router monitoring function.
*5: The HUB monitoring function can be used. Be sure to set this function when using the NIC switching function.
*6: The remote party is automatically identified in Fast switching mode and then monitored.
*7: When using GS/SURE linkage mode, be sure to set a function to monitor the other side to communicate.
*8: In Fast switching mode, only the dynamic adding/deleting function of real interfaces can be used.
*9: In NIC switching mode, only the dynamic switching function of interfaces used can be used.

2.2.1 Multiple virtual interface definition function

You can define and activate several virtual interfaces. This function extends the duplicating application range in a multi networks configuration. For details, see 3.2, "Setting, Changing, and Deleting Configuration Information"

Figure 2.24 below shows the concept of defining two virtual interfaces.

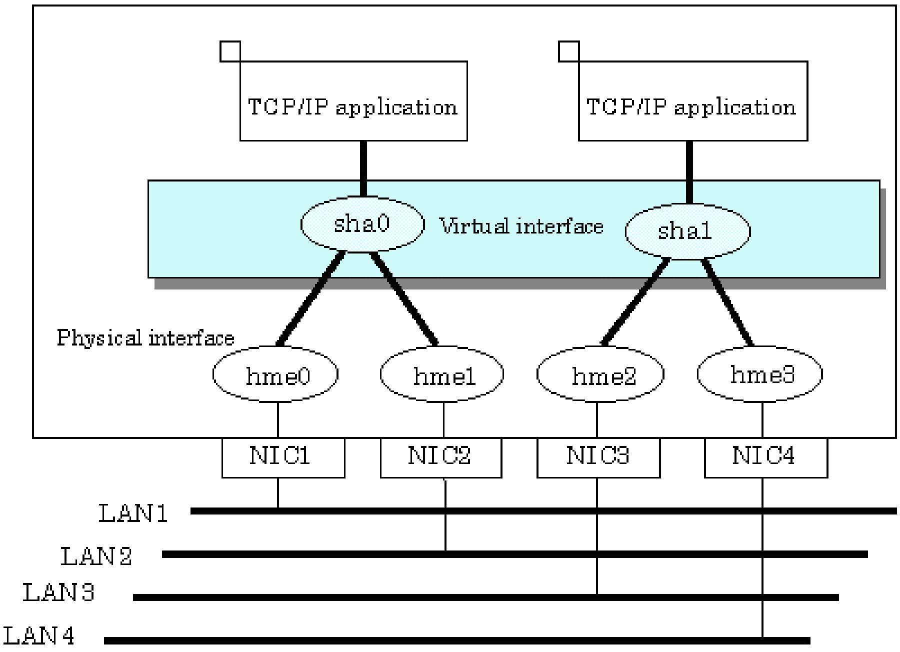


Figure 2.24 Two virtual interfaces being defined

2.2.2 Cluster failover function due to a transmission failure (inter-node job s witching)

In cluster operation, you can set whether or not to perform failover between clusters (switch jobs between nodes) if communication is disabled via all the physical interfaces bundled by a virtual interface. Selecting to "perform cluster failover upon a transmission failure" allows clusters to be switched without intervention of the system administrator if a line failure is detected. Cluster failover is enabled in the initial setup for duplicated path operation in Fast switching mode, NIC switching mode. For information on the setup, see Section 3.3.7.3, "Cluster failover (inter-node job switching) function". This function is automatically set when a cluster definition is made.

Figure 2.25 shows the concept of failover to a cluster service on node B when communication is disabled via both hme0 and hme1 bundled by virtual interface sha0 on node A.

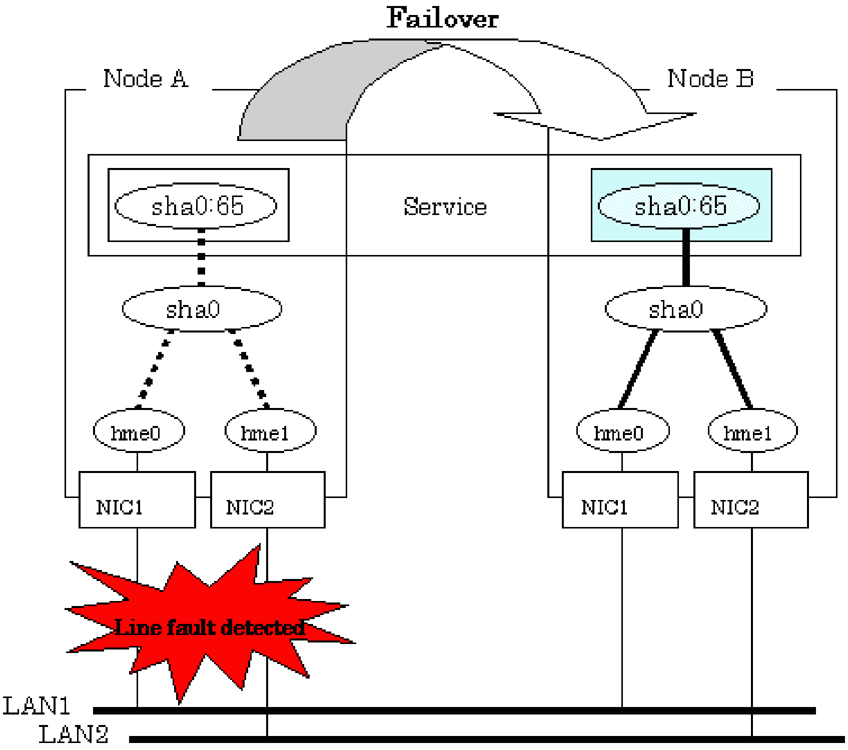


Figure 2.25 Cluster failover because of line fault

2.2.3 Concurrent operation function with other modes via one 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. For details, see 3.2, "Setting, Changing, and Deleting Configuration Information"

Figure 2.26 shows the concept of Fast switching/RIP mode operation.

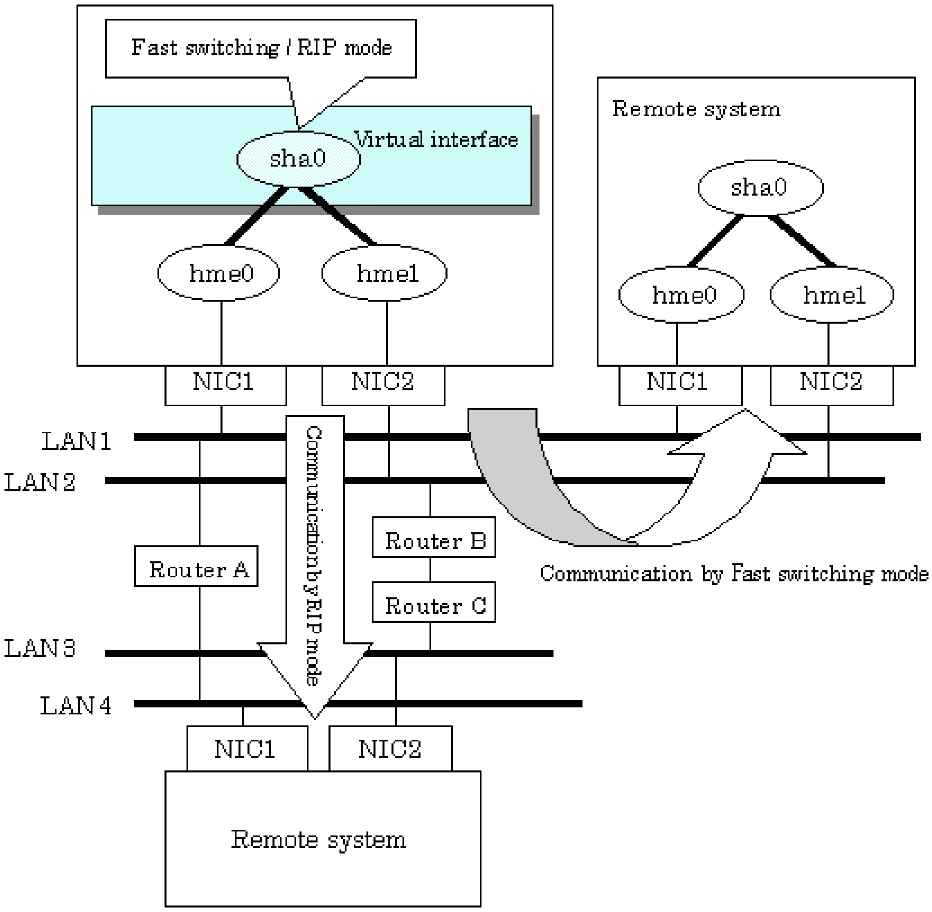


Figure 2.26 Fast switching/RIP mode operation

2.2.4 Sharing function of physical interface

Several virtual interfaces can share a single physical interface. Since the number of virtual interfaces sharing a single physical interface is not limited, resources can be shared effectively. In addition, you can set different operation configuration for each of the virtual interfaces sharing a single physical interface. For details, see 3.2, "Setting, Changing, and Deleting Configuration Information"

Figure 2.27 shows an example of virtual interfaces sha0 and sha1 sharing physical interface hme1.

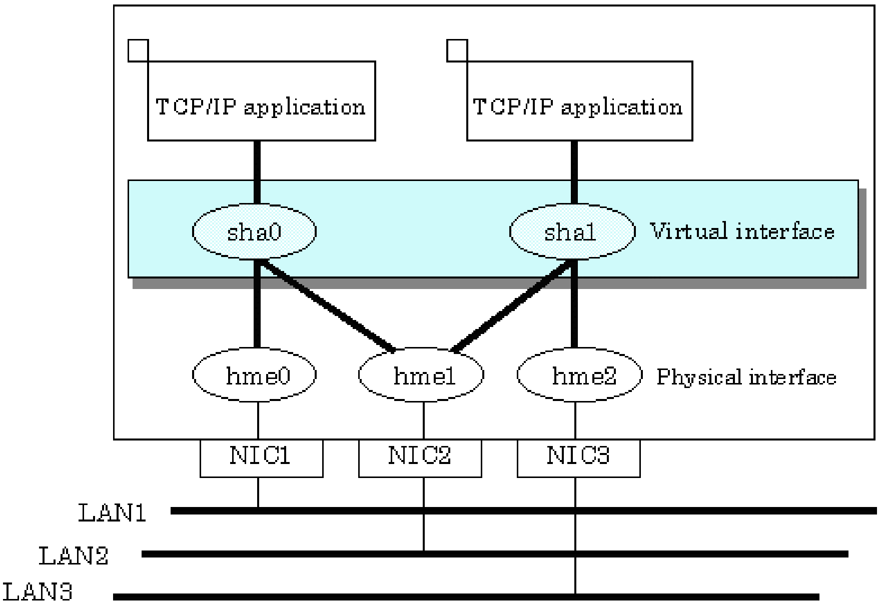


Figure 2.27 Physical interface being shared

2.2.5 Multiple logical virtual interface definition function

You can define several IP addresses (logical virtual interfaces) on a single virtual interface. The defined IP addresses can be used at the same time. This function enables IP addresses to be assigned without requiring additional physical interfaces. For details, see 3.2, "Setting, Changing, and Deleting Configuration Information"

Figure 2.28 shows an example of defining three logical virtual interfaces to virtual interface sha0.

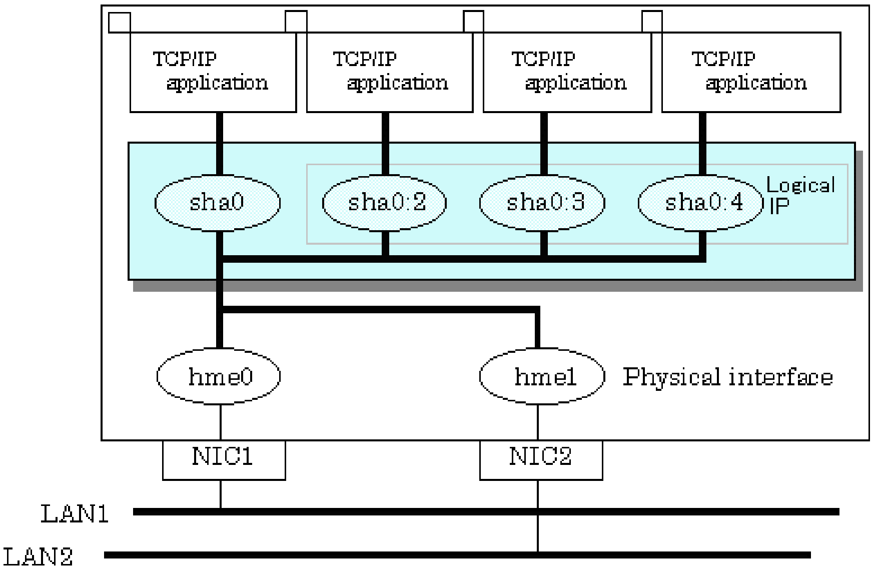


Figure 2.28 Logical virtual interface being defined

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

2.2.6 Single physical interface definition function

You can create a virtual interface, which has 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. For details, see 3.2, "Setting, Changing, and Deleting Configuration Information"

Figure 2.29 shows an example of single physical interface configuration.

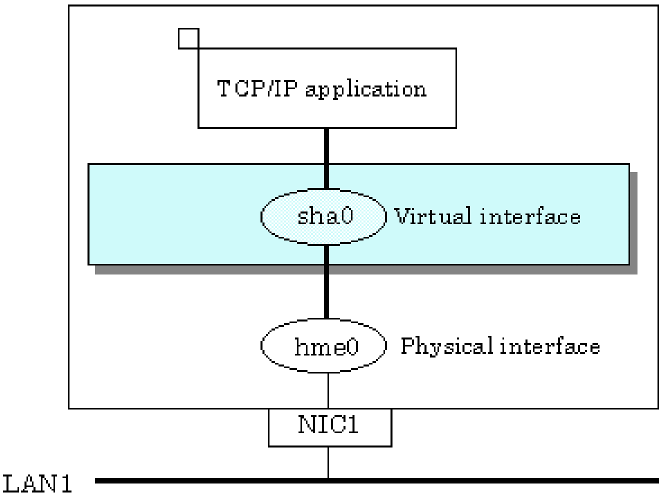


Figure 2.29 Single physical interface configuration

2.2.7 Message output function 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.

For details about the Fast switching mode, see 3.3.7, "Setting message output function in response to a transmission line failure."

For details about the RIP mode or NIC switching mode, see 3.3.8, "Setting Router/HUB monitoring function."

For details about GS/SURE linkage mode, see 3.3.9, "Setting communication party monitoring function."

2.2.8 Router/HUB monitoring function

Router monitoring function

The router monitoring function switches lines by issuing the ping command to neighboring routers (up to two routers can be registered per virtual interface) at regular intervals and restarting in.routed if a line failure is detected. If the router monitoring function is disabled, about five minutes are required to switch lines when a failure is detected on a line. If the router monitoring function is enabled, the switching time can be reduced to about one minute (depending on the setting). (The switching time may not be reduced if a routing daemon is active on another node on the same network or if a line failure occurs in an unfavorable location on the line.) Additionally, enabling the router monitoring function enables a message to be output if a line failure occurs. Figure 2.30 shows the outline of the router monitoring function. When the operation starts, this function performs ping monitoring on the primary monitored router (router A in the figure). When a failure is detected in the primary monitored router, the routing daemon is restarted. Then, this function stops monitoring the primary monitored router and starts monitoring the secondary monitored router (router B in the figure).

Routers can be connected only between different networks.

Traffic is controlled in accordance with the RIP information using a single transmission line.

For information on the setup, see Section 3.3.8, "Setting router/HUB monitoring function".

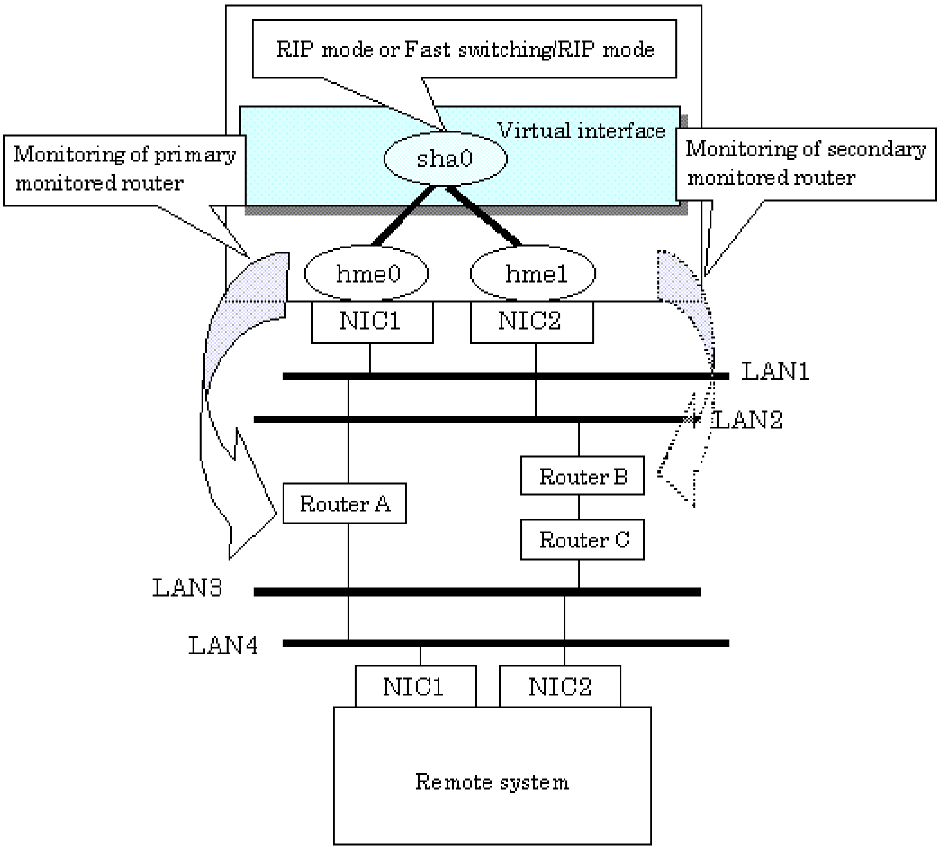

RIP mode or Fast switching/RIP mode
Virtual interface
Monitoring of primary monitored router
sha0
Monitoring of secondary monitored router
hme0
hme1
NIC1
NIC2
LAN1
LAN2
Router B
Router A
Router C
LAN3
LAN4
NIC1
NIC2
Remote system

Figure 2.30 Router monitoring function

HUB monitoring function

The HUB monitoring function issues the ping command to neighboring HUBs (up to two HUBs can be registered per virtual interface) at regular intervals and switches the interface to be used if a line failure is detected. This function can also monitor a line between two HUBs (inter-HUB monitoring function). This function can thus prevent a communication error from occurring due to NIC switching when an inter-HUB failure occurs. Figure 2.31 shows an outline of the HUB monitoring function.

If the operation starts without using the inter-HUB monitoring function, the primary HUB (HUB1 in the figure) 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 NIC of the current standby system is activated. After the standby NIC is activated, the secondary HUB (HUB2 in the figure) is monitored using the ping command. If the secondary HUB is faulty before switching and then a switching event occurs, communication after interface switching may not be executed normally.

If the operation starts using the inter-HUB monitoring function, the secondary HUB (HUB2 in the figure) is monitored using the ping command. When a failure is detected in the secondary HUB, the primary HUB (HUB1 in the figure) is monitored using the ping command. (At this point, a message is output, notifying that the monitoring of the secondary HUB has failed. Find the cause of the failure.) If, later, a failure is detected in the primary HUB, the NIC of the currently active system is inactivated and then the NIC of the current standby system is activated. After the standby NIC is activated, the primary HUB (HUB1 in the figure) is monitoring using the ping command. When a failure is detected in the primary HUB, the secondary HUB (HUB2 in the figure) is monitored using the ping command. Even if the secondary HUB is faulty before switching, recovery can be made before a switching event occurs because a message is output.

Be careful of the switching time setting (the product of values specified in the "-s" and "-c" options of the hanetpoll on command) because switching takes twice as long when the inter-HUB monitoring function is used as when it is not used. For information on the setup, see Section 7.7, "hanetpoll Command".

While the standby patrol function (see Section 2.2.10, "Standby patrol function") is used, the inter-HUB monitoring need not be used because the former serves also as the latter. For information on the setup, see Section 3.3.8, "Setting router/HUB monitoring function".

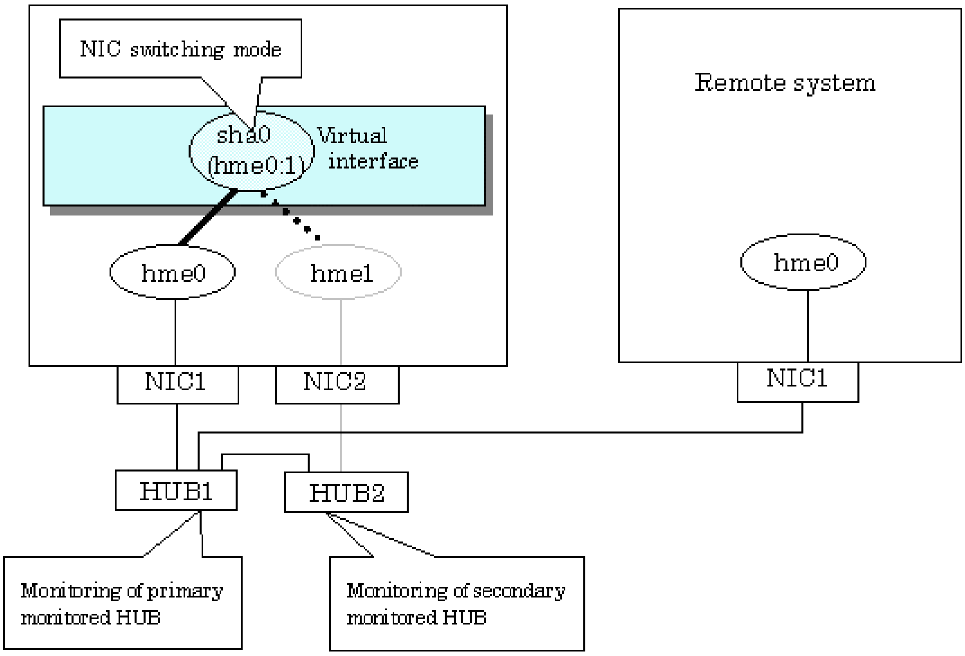


Figure 2.31 HUB monitoring function

2.2.9 Communication party monitoring function

In GS/SURE linkage mode, the ping command is issued to the IP address of the real interface of the communication party at regular intervals. If a line failure is detected, a message is output and communication continues using other transmission paths.

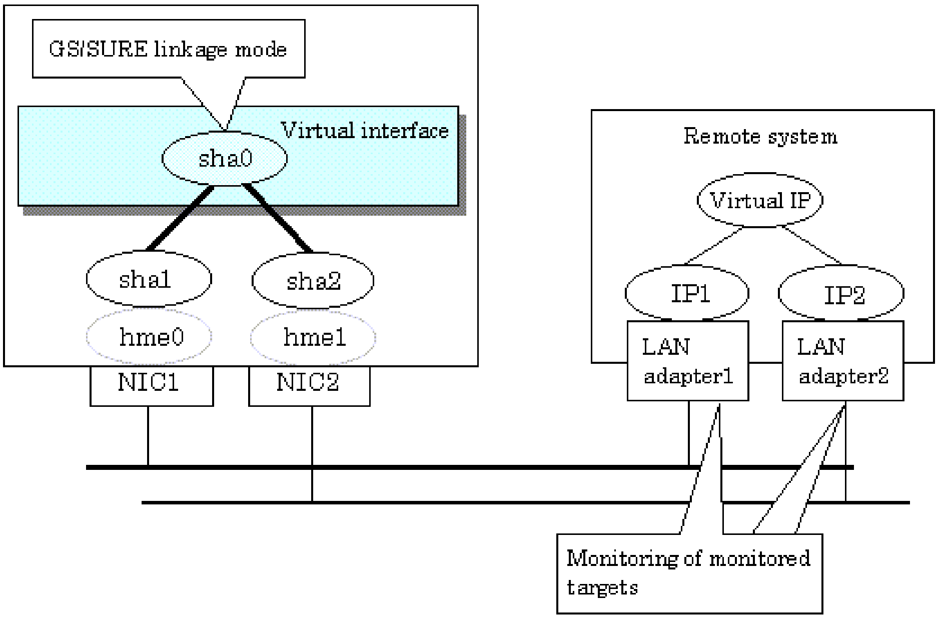


Figure 2.32 Communication party monitoring function

2.2.10 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:

- Outputs a message when an error occurred. This prevents switching beforehand when an error occurred in the actual interface of the present operation system, with an error had already occurred in the actual interface of a standby system.

- Possible to do failback automatically when the present NIC recovered after switched to a standby NIC at the time of an error.
- Resumes a function to monitor transfer routes automatically at the recovery of standby patrol when an error occurred in all transfer routes.

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. Possible to operate manually. See "7.10 The strptl command" for starting standby patrol manually and "7.11 The stpptl command" for stopping standby patrol.

See "3.3.10 The setting of a standby patrol function" for how to set standby patrol and "2.2.12 An automatic failback function" for an automatic failback function.

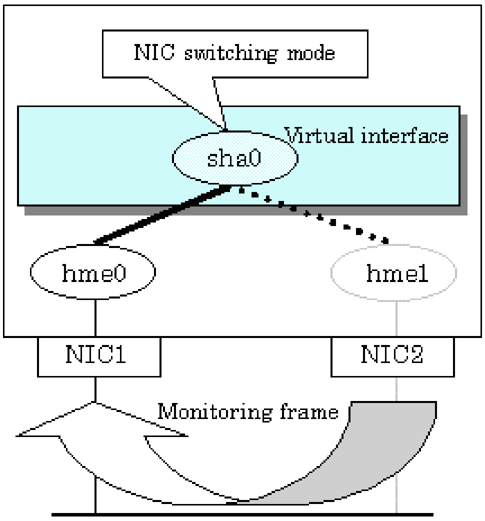


Figure 2.33 Standby patrol function

2.2.11 Dynamic adding/deleting/switching function of interfaces used

In Fast switching mode, RIP mode, Fast switching/RIP mode, and GS/SURE linkage mode (the operation mode is "c"), possible to add/delete bundled actual interfaces with a virtual interface kept activated (dynamic). The hanetnic command adds/deletes dynamically. See "7.9 hanetnic command" for the detail.
Figure 2.34 shows the outline of workings when executed a command to add/delete the actual interface dynamically.
There are following two modes in a command to add/delete the actual interface dynamically.

Temporal dynamic addition/deletion:

Operates actual interfaces to bundle without editing a configuration information file. Therefore, it automatically returns to the original state by operating a machine to reboot, etc. Not possible to add other than the actual 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. Not possible to delete permanently when a virtual interface is registered to the cluster resource.

In NIC switching mode, it is possible to make changes manually so that the standby real interface can be used while the currently operating interface is active (dynamic). Figure 2.35 shows an outline of operations performed when the real interface switching command is executed. For information on the setup, see Section 3.3.11, "Setting dynamic addition/deletion/switching function of real interfaces".

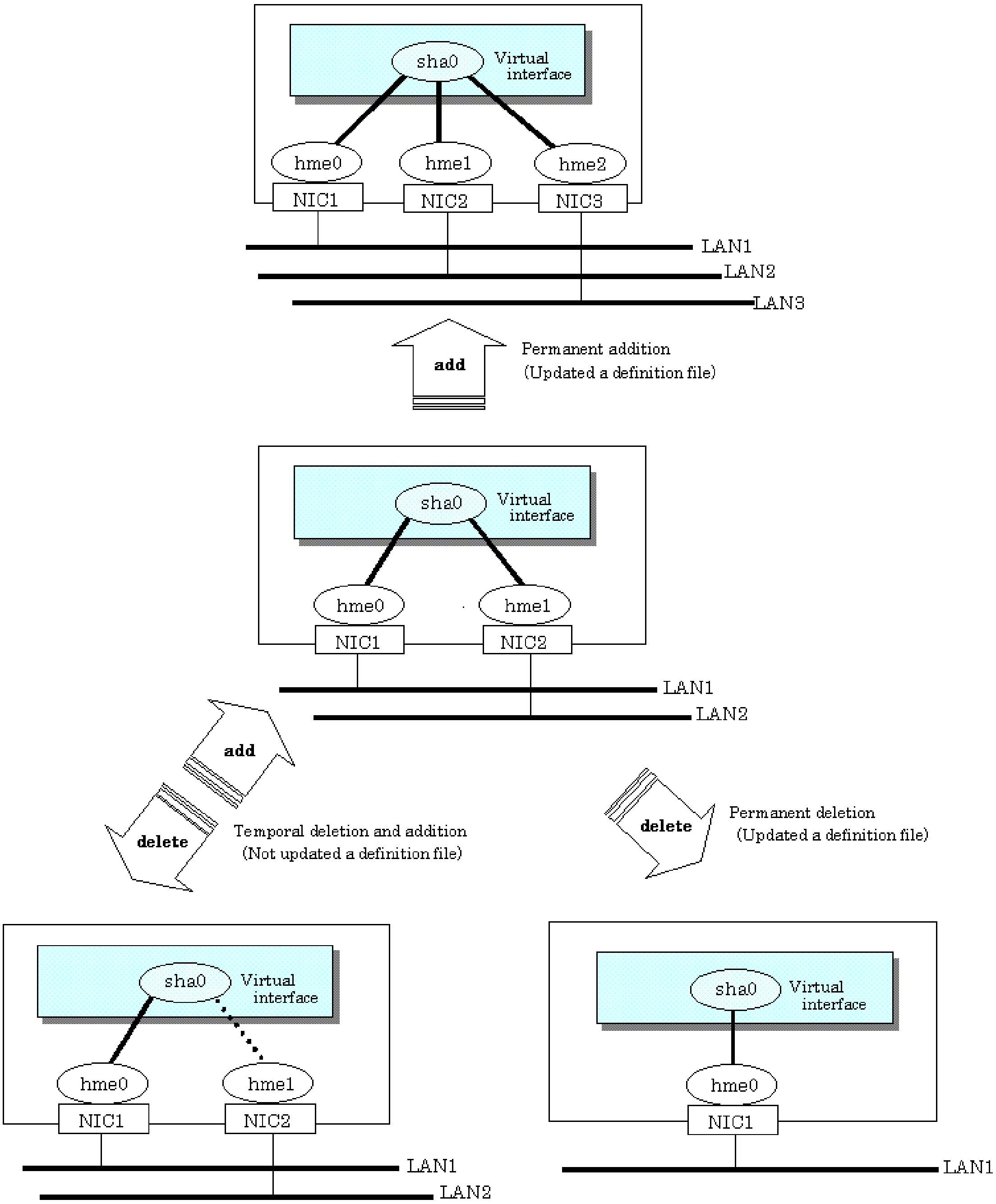

sha0
Virtual interface
hme0
hme1
hme2
NIC1
NIC2
NIC3
LAN1
LAN2
LAN3
add
Permanent addition
(Updated a definition file)
add
delete
Temporal deletion and addition
(Not updated a definition file)
delete
Permanent deletion
(Updated a definition file)

Figure 2.34 Dynamic adding/deleting function of interfaces used

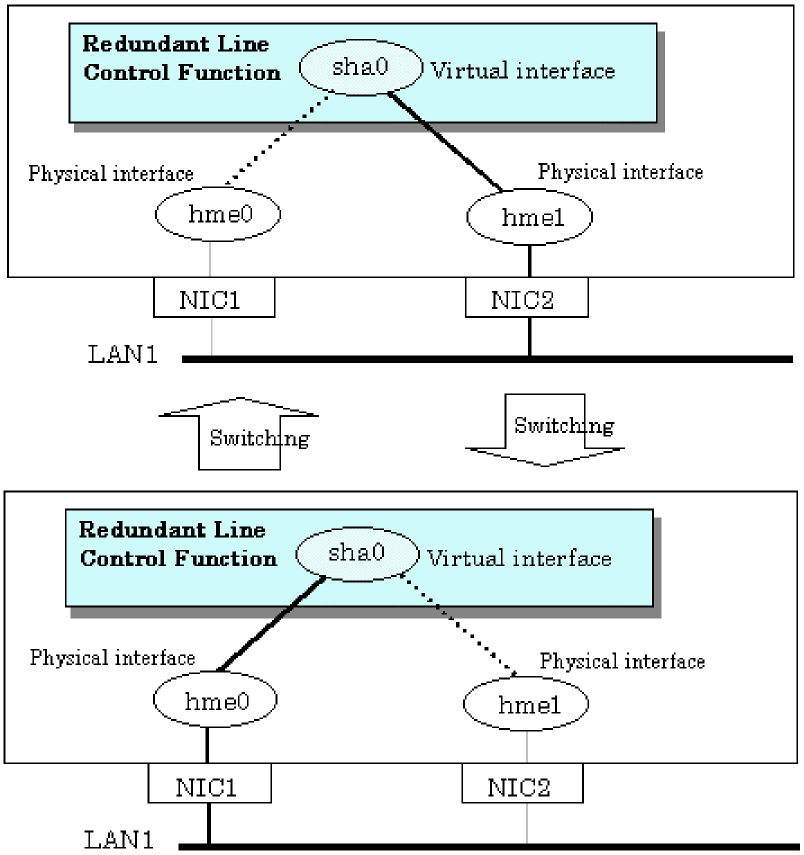


Figure 2.35 Dynamic switching function of interfaces used

2.2.12 Automatic failback function

In NIC switching mode, use the standby patrol function to "automatically perform failback immediately after the primary interface recovers" or "perform failback when the secondary interface currently used encounters a failure". For information on the setup, see Section 3.3.10, "Setting standby patrol function". Figure 2.36 shows the outline of the automatic failback function.

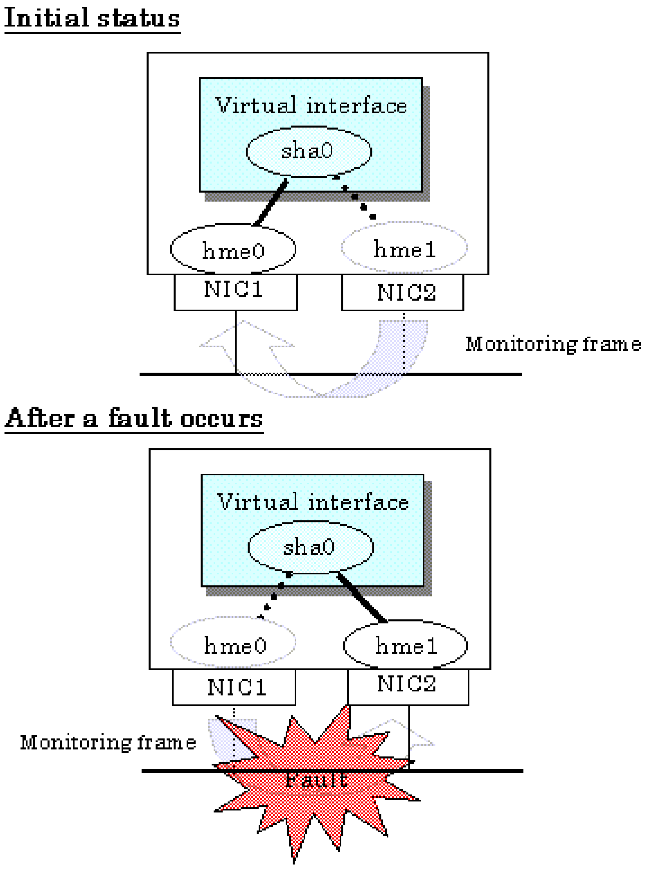


Figure 2.36 Automatic failback function (continued)

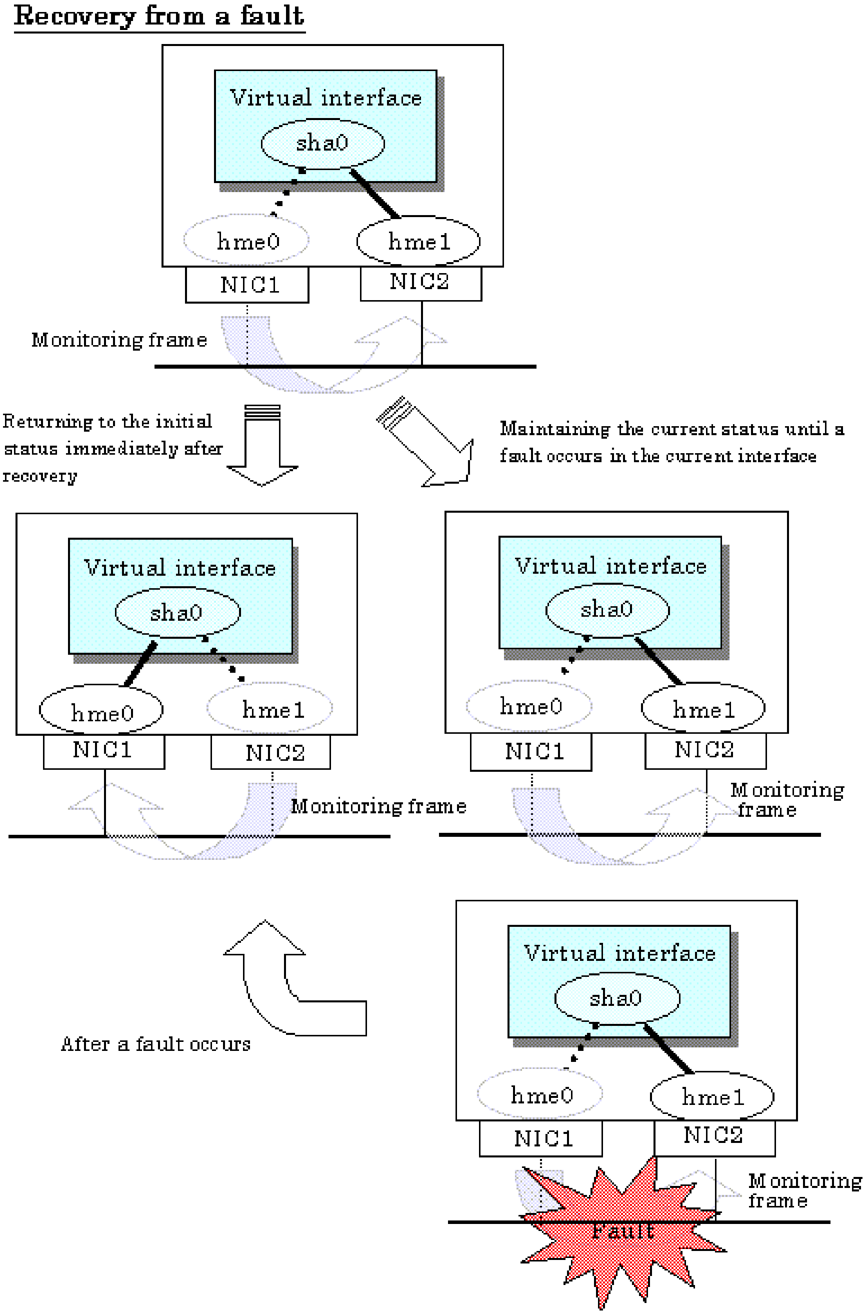


Figure 2.36 Automatic failback function (end)

When specified other than HUB as a monitor-to 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 monitor-to device to execute prompt failback.

2.2.13 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 3.3.12, "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 such as to reactivate an application after activated or deactivated an IP address, to set the specified routing information, to delete the ARP information, or 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 2.37 shows timing to run a user command when activated or deactivated an IP address in NIC switching mode (a logical IP address takeover function).

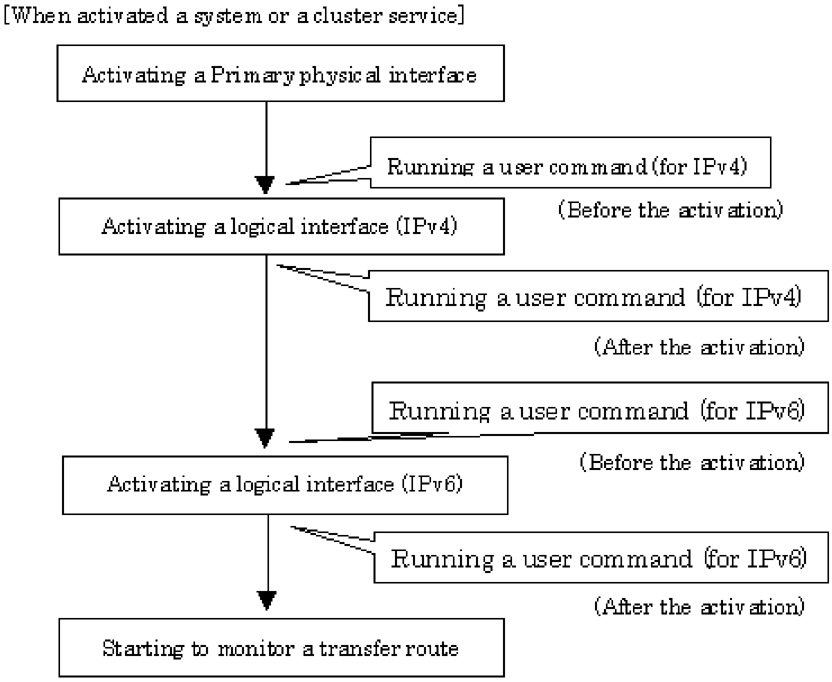

[When activated a system or a cluster service]
Activating a Primary physical interface
Running a user command (for IPv4)
(Before the activation)
Activating a logical interface (IPv4)
Running a user command (for IPv4)
(After the activation)
Running a user command (for IPv6)
(Before the activation)
Activating a logical interface (IPv6)
Running a user command (for IPv6)
(After the activation)
Starting to monitor a transfer route

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

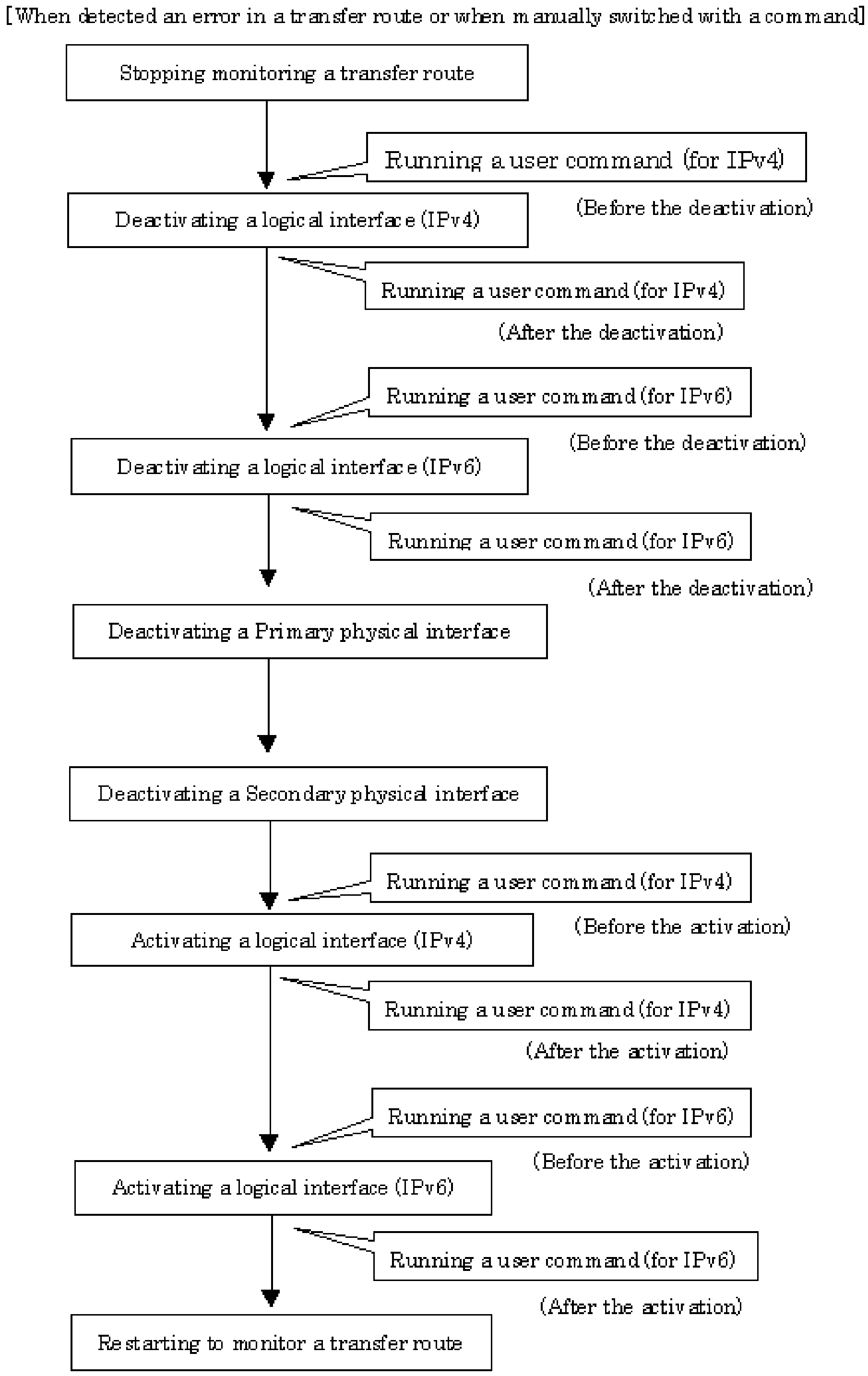

[When detected an error in a transfer route or when manually switched with a command]
Stopping monitoring a transfer route
Running a user command (for IPv4)
(Before the deactivation)
Deactivating a logical interface (IPv4)
Running a user command (for IPv4)
(After the deactivation)
Running a user command (for IPv6)
(Before the deactivation)
Deactivating a logical interface (IPv6)
Running a user command (for IPv6)
(After the deactivation)
Deactivating a Primary physical interface
Deactivating a Secondary physical interface
Running a user command (for IPv4)
(Before the activation)
Activating a logical interface (IPv4)
Running a user command (for IPv4)
(After the activation)
Running a user command (for IPv6)
(Before the activation)
Activating a logical interface (IPv6)
Running a user command (for IPv6)
(After the activation)
Restarting to monitor a transfer route

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

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

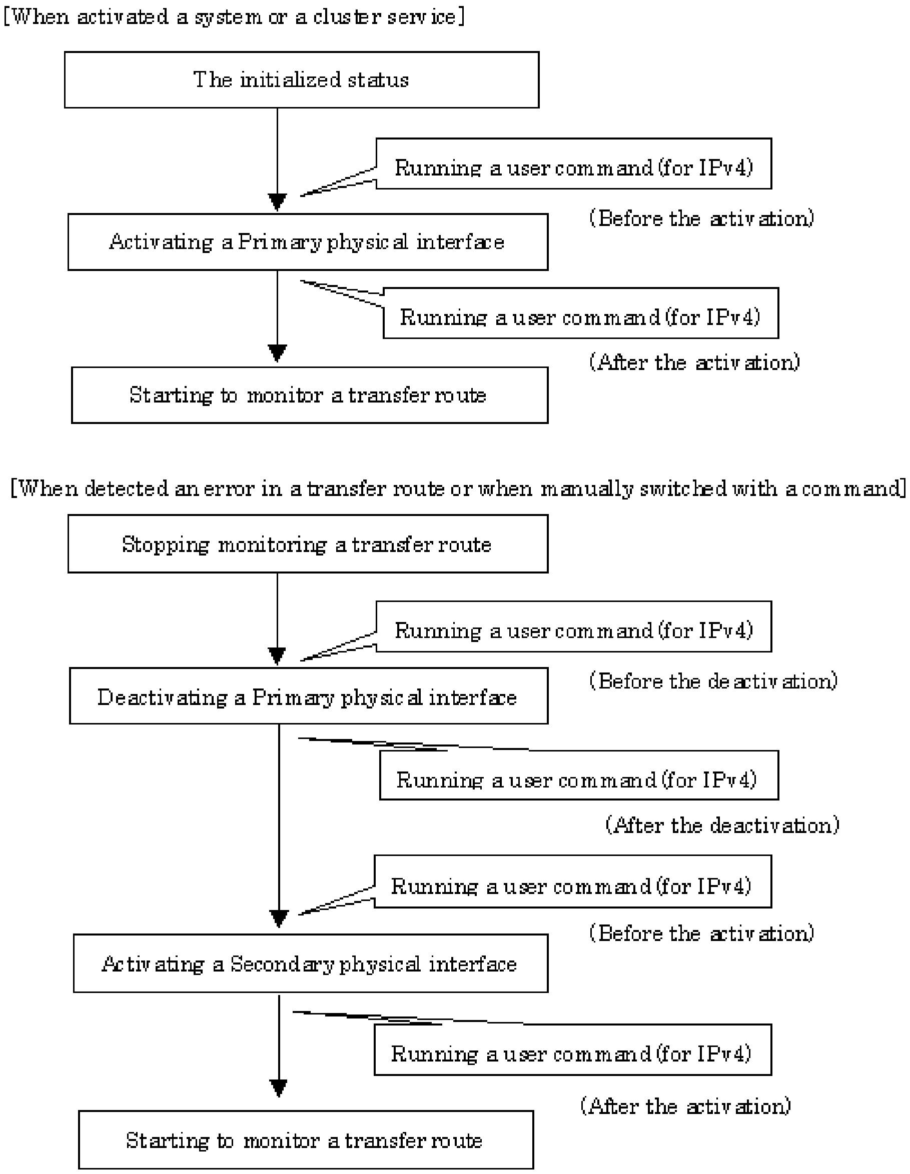

[When activated a system or a cluster service]
The initialized status
Running a user command (for IPv4)
(Before the activation)
Activating a Primary physical interface
Running a user command (for IPv4)
(After the activation)
Starting to monitor a transfer route
[When detected an error in a transfer route or when manually switched with a command]
Stopping monitoring a transfer route
Running a user command (for IPv4)
(Before the deactivation)
Deactivating a Primary physical interface
Running a user command (for IPv4)
(After the deactivation)
Running a user command (for IPv4)
(Before the activation)
Activating a Secondary physical interface
Running a user command (for IPv4)
(After the activation)
Starting to monitor a transfer route

Figure 2.38 Timing to run a user command when activated or deactivated an IP address (a physical IP address takeover function)

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

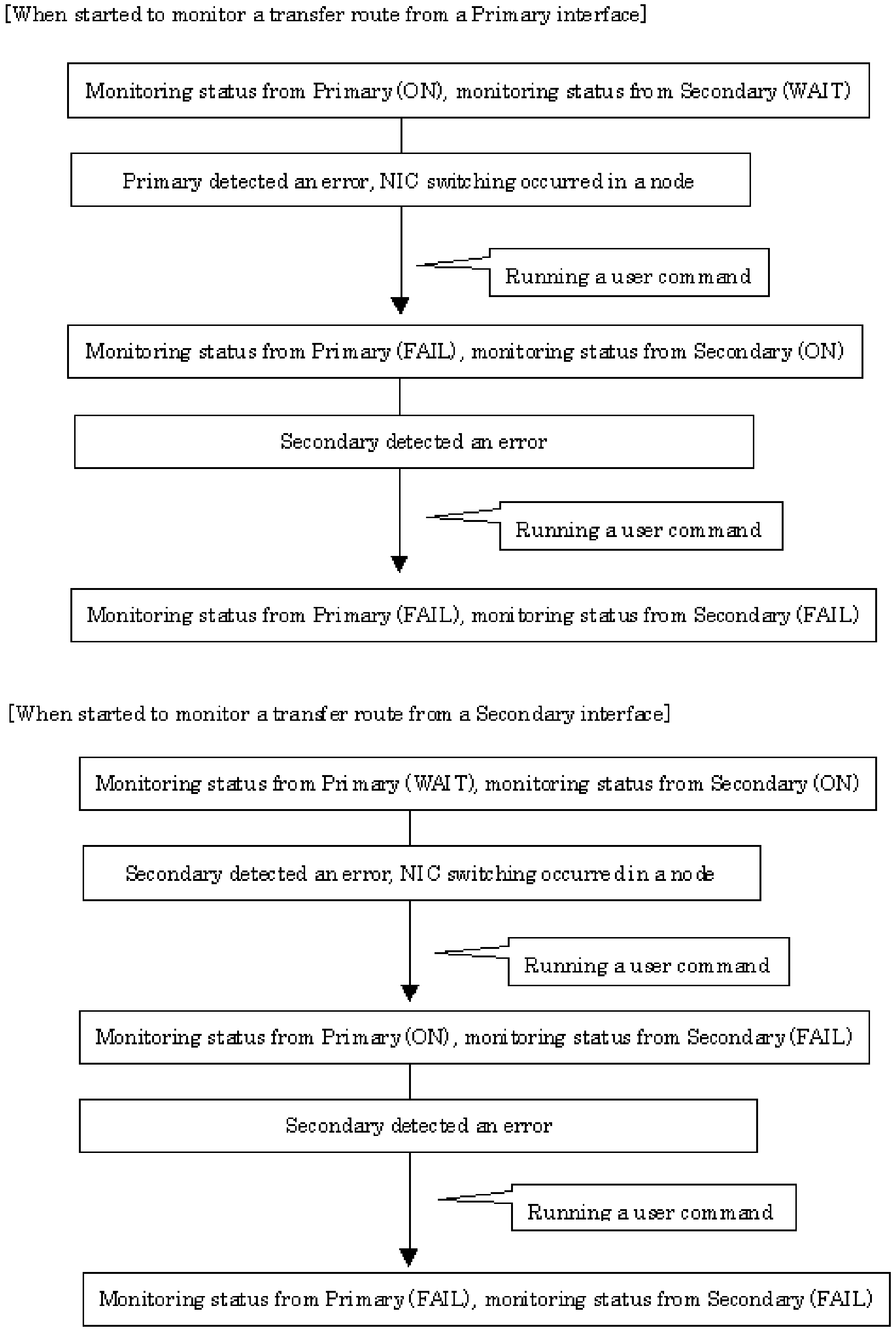

[When started to monitor a transfer route from a Primary interface]
Monitoring status from Primary (ON), monitoring status from Secondary (WAIT)
Primary detected an error, NIC switching occurred in a node
Running a user command
Monitoring status from Primary (FAIL), monitoring status from Secondary (ON)
Secondary detected an error
Running a user command
Monitoring status from Primary (FAIL), monitoring status from Secondary (FAIL)
[When started to monitor a transfer route from a Secondary interface]
Monitoring status from Primary (WAIT), monitoring status from Secondary (ON)
Secondary detected an error, NIC switching occurred in a node
Running a user command
Monitoring status from Primary (ON), monitoring status from Secondary (FAIL)
Secondary detected an error
Running a user command
Monitoring status from Primary (FAIL), monitoring status from Secondary (FAIL)

Figure 2.39 Timing to run a user command when detected an error in a transfer route

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

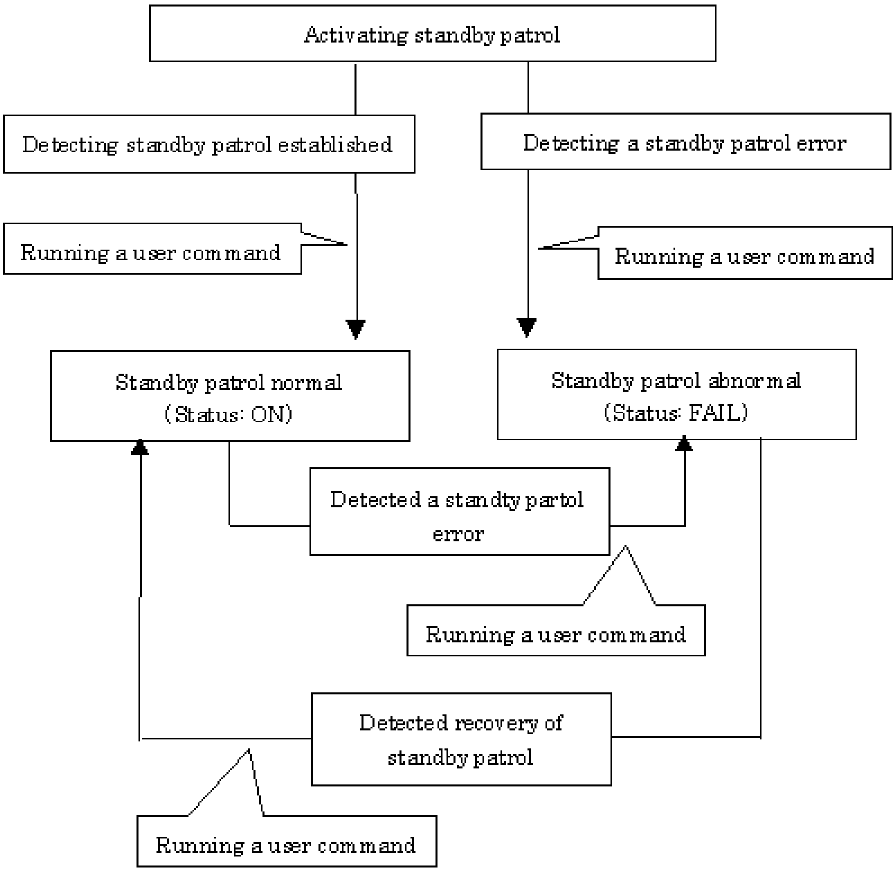

Activating standby patrol
Detecting standby patrol established
Detecting a standby patrol error
Running a user command
Running a user command
Standby patrol normal
(Status: ON)
Standby patrol abnormal
(Status: FAIL)
Detected a standty partol error
Running a user command
Detected recovery of standby patrol
Running a user command

Figure 2.40 Running a user command when detected a standby patrol error or recovery

(2) GS/SURE linkage mode

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

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

[When the other system hot standby switched]

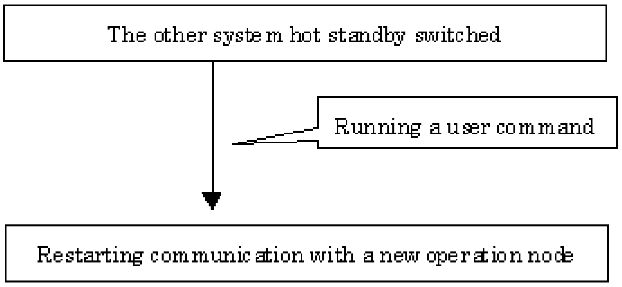

The other system hot standby switched
Running a user command
Restarting communication with a new operation node

Figure 2.41 Timing to run a user command when the other system hot standby switched

2.2.14 DR (Dynamic Reconfiguration) linkage function

Possible to use a DR (Dynamic Reconfiguration) function ("a DR function") provided by GP7000F M1000/2000 and

PRIMEPOWER 800/1000/2000. (However, it is not possible to use this DR function when defined IPv6 to a virtual interface in NIC switching mode.)
See the following manuals to use a DR function.

- Dynamic Reconfiguration Architecture Guide
- Dynamic Reconfiguration Users Guide

A DR linkage script is provided to realize DR in a Redundant Line Control Function. Therefore, a DR linkage 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 linkage script used in various modes. "Figure 2.42 The outline of the workings of DR" shows a flow of exchanging system boards (SB) using a DR function.

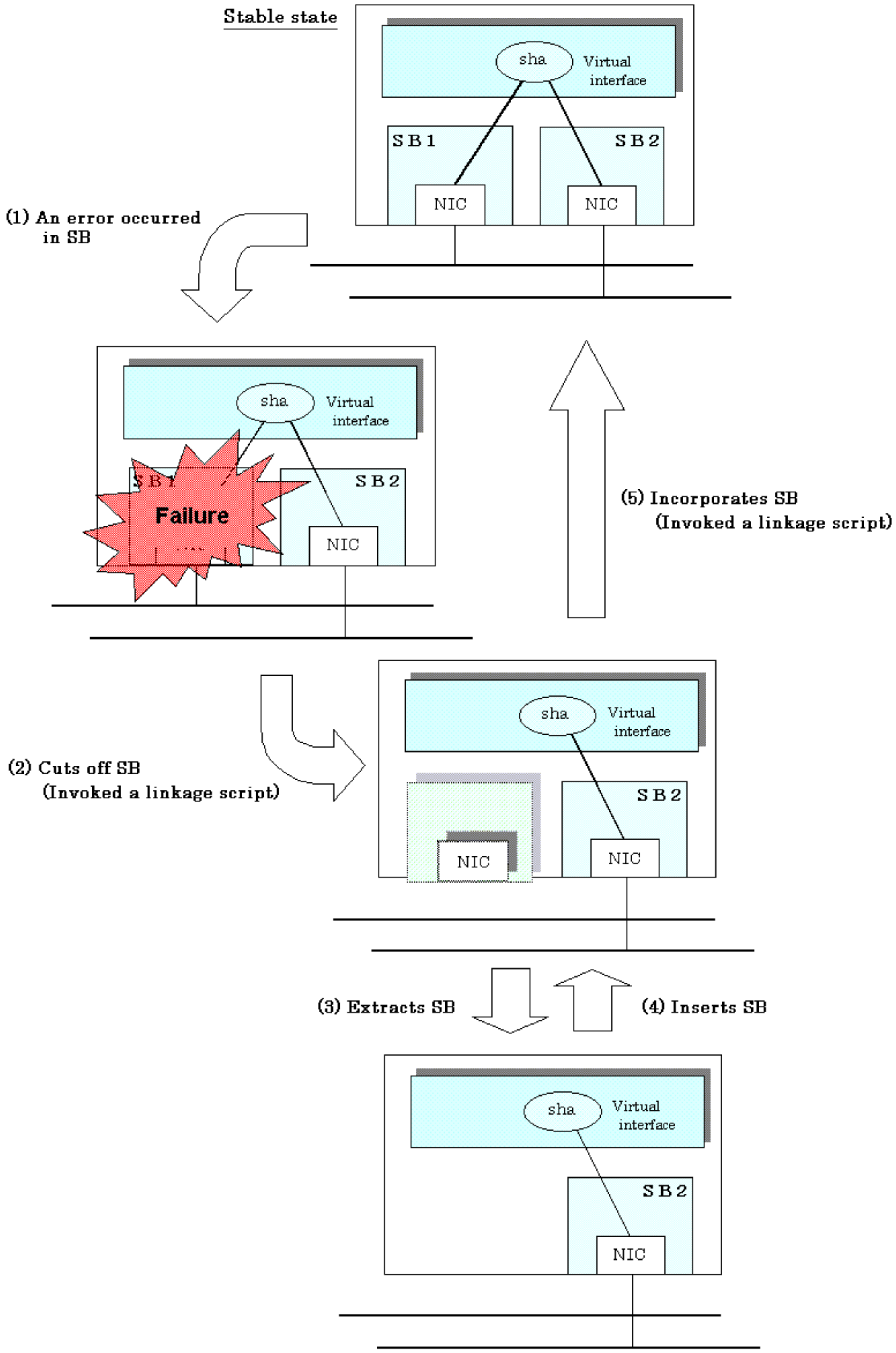


Figure 2.42 The outline of the workings of DR

2.3 Notes

2.3.1 General

Notes on setting an configuration:

- The maximum number of definitions for virtual and logical virtual interfaces is a total of 64.
- The number of physical interfaces in a single virtual interface is from 1 to 8.
- The maximum number of logical virtual interfaces that can be defined to a single logical virtual interface is 63.
- All host names and IP addresses to use in a Redundant Line Control Function must be linked in /etc/inet/hosts and /etc/inet/ipnodes files of the own system.

Notes on the operation:

- 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.
- Not possible to use a Redundant Line Control Function under the subnet environment of the variable length. Not possible to get the route information dynamically under the subnet environment of the variable length because in.routed of Solaris 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.
  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.

Notes on upper applications:

- When using TCP protocol 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 protocol. Necessary to execute a recovery process such as sending the data by the application itself.
- 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.

2.3.2 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. 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 VALN (Virtual LAN), occasionally 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.

2.3.3 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, some time is required to modify the path information between routers (about 5 minutes if the router polling 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. 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.

2.3.4 Duplicated operation by Fast switching/RIP mode

- 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.

2.3.5 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-HUB connection and then connect the cable to each HUB (See "Figure 2.13 System configuration in NIC switching mode" of "2.1.3 NIC switching mode").
- 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, 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 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, necessary to use HUB possible to set an IP address because ping monitors an error. When not possible to set an IP address, it is also possible to use an IP address of the other device connected to HUB. However, when the device itself caused an error, it is processed as an error of a transfer route. Pay attention to this matter.
- 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.

2.3.6 Duplicated operation via GS/SURE linkage mode

- In GS/SURE linkage mode, the system uses duplicated paths concurrently but this cannot be expected 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.
- Not possible to have GS/SURE linkage method and RIP method at the same time on the same system.
- Not possible to use GS/SURE linkage method for the communication with PRIMEPOWER, GP7000F.
- When switched a cluster on the PRIMEPOWER, GP7000F side, 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, necessary to release in each TCP application to recover the communication.

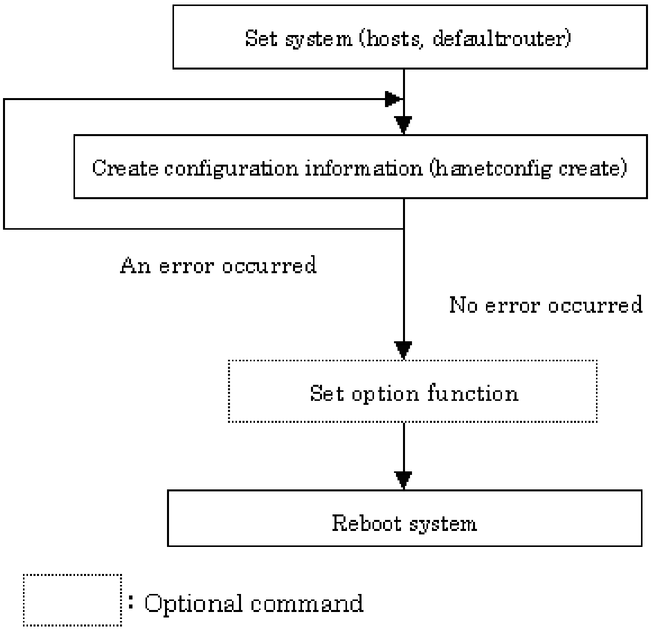
Chapter 3 Installation

This chapter explains how to setting up Redundant Line Control Function.

3.1 System Setup

This section explains how to set up the system to use Redundant Line Control Function. For more information, see the manuals of Solaris.

The following is setting up procedure:



Set system (hosts, defaultrouter)
Create configuration information (hanetconfig create)
An error occurred
No error occurred
Set option function
Reboot system
: Optional command

Figure 3.1 Redundant Line Control Function setting procedure

3.1.1 Setup common to modes

- When added NIC to a device of the body, first have a device of the body recognize the added NIC by such as executing boot -r command from the ok prompt and activating a system, then set a virtual interface.
- 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 other name services such as DNS operation and NIS operation, define to refer a local file first (/etc/nsswitch.conf file) for a keyword of hosts and netmasks. (This makes an address solution end normally even when not possible to communicate with DNS server or NIS server.)
- When using an IPv6 address, define an IPv6 address and a host name to set to the environment definition in an /etc/inet/ipnodes file. When using the other name service such as DNS or NIS operations, define to refer a local file first in an ipnodes keyword (/etc/nsswitch.conf file).
- Not possible to change the information corresponding to the host name specified at the environment setting of a Redundant Line Control Function (the information of a host name on the host database of such as /etc/inet/hosts file)after defined the environment of a Redundant Line Control Function. To change the information on the host database of such as /etc/inet/hosts file, it is necessary to delete various definitions of a Redundant Line Control Function and to set the definition again.

For more information, see the manuals of Solaris.

3.1.2 System setup in Fast switching mode

- As for an actual interface to configure, 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.)

3.1.3 System setup in RIP mode

- Set to activate a routing daemon because it is necessary to change the route information dynamically. (Do not create /etc/defaultrouter and /etc/notrouter files. Check if or not a file exists, and change a name or delete it if exists.)

- 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.
- As for an actual interface to configure, 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.)

3.1.4 System setup in Fast switching/RIP mode

- Set to activate a routing daemon because it is necessary to change the route information dynamically. (Do not create /etc/defaultrouter and /etc/notrouter files. Check if or not a file exists, and change a name or delete it if exists.)
- 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.
- As for an actual interface to configure, 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.)

3.1.5 System setup in NIC switching mode

- 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 an IPv6 address, define a configured actual interface to use in IPv6 before defining a virtual interface. (Check if or not there is an /etc/hostname6.interface file. If not, create it and reboot. When creating a /etc/hostname6.interface file, make it empty without fail.)
- 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. 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 on    # 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".
```

3.1.6 System setup in GS/SURE linkage mode

- Create an /etc/notrouter file.
- Do not create an /etc/defaultrouter file because path information must be dynamically changed. (Check for the existence of an /etc/defaultrouter file and, if one exists, rename or delete it.)
- 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.
- The actual interface to be specified must not be defined for normal use in 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.)

3.2 Setting, Changing, and Deleting Configuration Informat ion

3.2.1 Setting configuration information

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

3.2.1.1 Adding configuration information for 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. Set up a virtual interface using the hanetconfig create command. When sharing NIC in more than one interface, at setting a virtual interface of the second and after, specify a physical interface of the same name as that of a physical interface which is used by the previously set virtual interface. Then execute hanetconfig create command.
   For information, see Section 7.1, "hanetconfig Command".

3.2.1.2 Adding configuration information for 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. Set up a virtual interface using the hanetconfig create command. When sharing NIC in more than one interface, at setting a virtual interface of the second and after, specify a physical interface of the same name as that of a physical interface which is used by the previously set virtual interface. Then execute 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".

3.2.1.3 Adding configuration information for 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. Set up a virtual interface using the hanetconfig create command. When sharing NIC in more than one interface, at setting a virtual interface of the second and after, specify a physical interface of the same name as that of a physical interface which is used by the previously set virtual interface. Then execute 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".

3.2.1.4 Adding configuration information for 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.

Notes)

When setting the definition information of NIC switching mode, if virtual interfaces of the other NIC switching modes are already working, necessary to stop them once to make the added information valid. Therefore, deactivate temporarily using a stphanet command and execute a strhanet command. In cluster operation, reactivate a cluster service of NIC switching mode.

3.2.1.5 Adding configuration information for 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".
3. Reboot the system.

3.2.2 Changing configuration information

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

3.2.2.1 Changing configuration information for 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, not necessary to reactivate a virtual interface. The information becomes valid immediately after changed.

The following lists the information that can be changed for Fast switching mode. No other information than listed below can be changed. Delete the concerned definition and make a definition 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".
  - Cycle in which the communication party should be monitored
  - Monitoring retry count until a message is output
  - Whether the inter-cluster failover (inter-node job switching) function is used

3.2.2.2 Changing configuration information for 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 other information than listed below can be changed. Delete the concerned definition and make a definition 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 hanetpoll command to change the following information. For information, see Section 7.7, "hanetpoll Command".
  - Monitored party information
  - Cycle in which the communication party should be monitored
  - Monitoring retry count until a message is output
  - Retry count at which router monitoring is stopped
  - Recovery monitoring interval
  - Whether the inter-cluster failover (inter-node job switching) function is used

3.2.2.3 Changing configuration information for 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 3.2.2.1, "Changing configuration information for Fast switching mode" and 3.2.2.2, "Changing configuration information for RIP mode".

3.2.2.4 Changing configuration information for 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 a function to monitor router/HUB using a 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 configuration information and the other information. (To change the information of a monitoring

function (interval to monitor, the number of the times to monitor, interval to monitor the recovery, failover function between clusters, workings when switching between nodes occurred due to an error of a transfer route during the cluster operation, and time to wait for HUB to link up after started monitoring), change them when executing a hanetpoll on command. See "7.7 hanetpoll Command" for the detail.

4. Deactivate temporarily all virtual interfaces set in NIC switching mode using a stphanet command, then reactivate them using a strhanet command. See "7.2 strhanet command" and "7.3 stphanet command" for the detail.
5. Starts a function to monitor router/HUB using a hanetpoll on command. (This changes the information of a monitoring function (interval to monitor, the number of the times to monitor, interval to monitor the recovery, failover function between clusters, workings when switching between nodes occurred due to an error of a transfer route during the cluster operation, and time to wait for HUB to link up after started monitoring) by an option of a hanetpoll on command. See "7.7 hanetpoll Command" for the detail.

The procedure to change only the monitoring information is as follows:

1. Stop a function to monitor router/HUB using a hanetpoll off command. See "7.7 hanetpoll Command" for the detail.
2. Start a function to monitor router/HUB using a hanetpoll on command. (This changes the information of a monitoring function (interval to monitor, the number of the times to monitor, interval to monitor the recovery, failover function between clusters, workings when switching between nodes occurred due to an error of a transfer route during the cluster operation, and time to wait for HUB to link up after started monitoring) by an option of a hanetpoll on command. Change the other information by "the procedure to change the configuration information, and the configuration information and the other 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 other information than listed below can be changed. Delete the concerned definition and make a definition 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 real interface
  - Interface names to be bundled by a virtual interface
- Monitoring function information
  Use the hanetpoll command to change the following information. For information, see Section 7.7, "hanetpoll Command".
  - Monitored party information
  - Primary and secondary HUB monitoring mode (if multiple parties are specified in monitoring destination information)
  - Cycle in which the communication party should be monitored
  - Monitoring retry count until a message is output
  - Recovery monitoring interval
  - Whether the inter-cluster failover (inter-node job switching) function is used
  - Wait time required until the HUB links up after monitoring is started
- 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
- Standby patrol information
  Use the hanetparam command to change the following information. For information, see Section 7.6, "hanetparam Command".
  - Cycle in which the communication party should be monitored
  - Monitoring retry count until a message is output

3.2.2.5 Changing configuration information for 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 information, see Section 7.3, "stphanet Command".
2. Stop the router/HUB monitoring function using the hanetpoll off command. For information, see Section 7.7, "hanetpoll Command".
3. Change the configuration information.
4. Reboot the system. (Note that you need restart only the monitoring function (hanetpoll off and on) to enable the setting if only the monitoring function information "monitoring interval, monitoring count, recovery monitoring interval, and inter-cluster failover function".)

The following lists the information that can be changed for GS/SURE linkage mode. No other information than listed below can be changed. Delete the concerned definition and make a definition 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 real interface
  - Interface names to be bundled by a virtual interface
- Monitoring function information
  Use the hanetpoll command to change the following information. For information, see Section 7.7, "hanetpoll Command".
  - Cycle in which the communication party should be monitored
  - Monitoring retry count until a message is output
  - Recovery monitoring interval
  - Whether the inter-cluster failover (inter-node job switching) function is used
- Monitored remote system information
  Use the hanetobserv command to change the following information. For information, see Section 7.5, "hanetobserv Command".
  - Identification name by which to identify the node of the communication party
  - Host name or IP address of a virtual interface owned by the communication party
  - Host name or IP address of real interface to be bundled by a virtual interface
  - Monitoring mode for a virtual interface of the specified monitoring destination
  - Communication party and destination network information with which communication should be performed using the relay destination virtual interface (only if the TCP relay function is used)

3.2.2.6 Note on changing configuration information

The following shows a note on changing configuration information.

- Not possible to change the configuration information of a virtual interface registered to the cluster resource. Necessary to delete the resource of a virtual interface registered to the cluster resource temporarily and register again after changed the configuration information.

3.2.3 Deleting configuration information

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

3.2.3.1 Deleting configuration information for Fast switching mode

The following shows the procedure for deleting 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. Delete the configuration information of the concerned virtual interface. For information, see Section 7.1, "hanetconfig Command".

3.2.3.2 Deleting configuration information for RIP mode

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

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".

3.2.3.3 Deleting configuration information for Fast switching/RIP mode

The following shows the procedure for deleting configuration information for Fast switching/RIP mode:

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".

3.2.3.4 Deleting configuration information for NIC switching mode

The following shows the procedure for deleting configuration information for NIC switching mode:

1. Stop the router/HUB monitoring function using the hanetpoll off command. 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 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. Reboot the system.

3.2.3.5 Deleting configuration information for GS/SURE linkage mode

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

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 all the 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. Reboot the system.

3.2.3.6 Note on deleting configuration information

The following shows a note on deleting configuration information.

- No virtual interface registered in the cluster resource can be deleted. Before doing so, you must delete the resource of the virtual interface registered in the cluster resource.

3.3 Setting Option Function

3.3.1 Setting multiple virtual interface setting function

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

3.3.2 Setting failover function because of a transmission line failure

Use the hanetparam command to set the failover function when a line failure occurs in Fast switching mode. For information on the setup, see Section 3.3.7.3, "Cluster failover (inter-node job switching) function".

Use the hanetpoll command to set the failover function when a line failure occurs in NIC switching mode. For information on the setup, see Section 3.3.8, "Setting Router/HUB monitoring function".

Use the hanetpoll command to set a failover function when an error occurred at a transfer route in NIC switching mode. Set a standby patrol function by the hanetconfig command when using an Automatic failback function. See "3.3.8 Setting Router/HUB monitoring function" and "3.3.10 Setting standby patrol function" as to how to set them.

Use the hanetobserv command to set the failover function when a line failure occurs in GS/SURE linkage mode. For details about this command, see Section 3.3.9, "Setting communication party monitoring function".

3.3.3 Setting concurrent operation function with other modes by using one vi rtual 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".

3.3.4 Setting physical interface sharing function

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".

3.3.5 Setting multiple logical virtual interface definition function

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".

3.3.6 Setting single physical interface definition function

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".

3.3.7 Setting message output function in response to a transmission line fail ure

Set the monitoring functions that can be specified for the operation in Fast switching mode. For details about RIP mode or NIC switching mode, see Section 3.3.8, "Setting Router/HUB monitoring function". For details about GS/SURE linkage mode, see Section 3.3.9, "Setting communication party monitoring function".

3.3.7.1 Setting transmission line monitor interval

Use the hanetparam command to set the line monitor interval. For details about this command, see Section 7.6, "hanetparam Command".

3.3.7.2 Enabling and disabling error message output function at transmission line failure

Specify the consecutive failure count for communication party monitoring before a message is output. Use the hanetparam command to set the count. For details about this command, see Section 7.6, "hanetparam Command".

3.3.7.3 Cluster failover (inter-node job switching) function

Specify the count of consecutive communication failures with the communication party before the failover (job switching between nodes) is performed in a cluster system. Use the hanetparam command to set the count. For details about this command, see Section 7.6, "hanetparam command".

3.3.8 Setting 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:

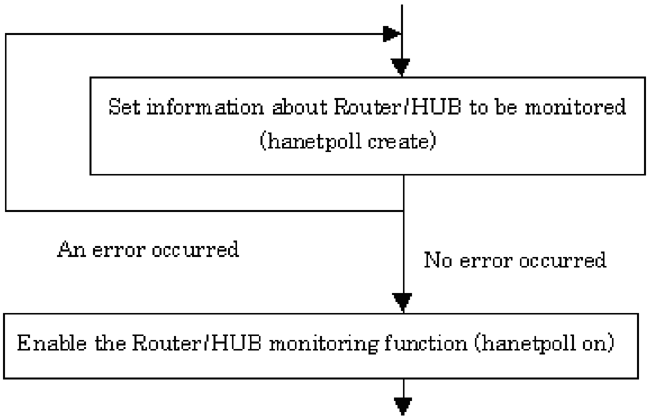

Set information about Router/HUB to be monitored
(hanetpoll create)
An error occurred
No error occurred
Enable the Router/HUB monitoring function (hanetpoll on)

Figure 3.2 Setting procedure of the Router/HUB monitoring function

3.3.8.1 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".

3.3.8.2 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".

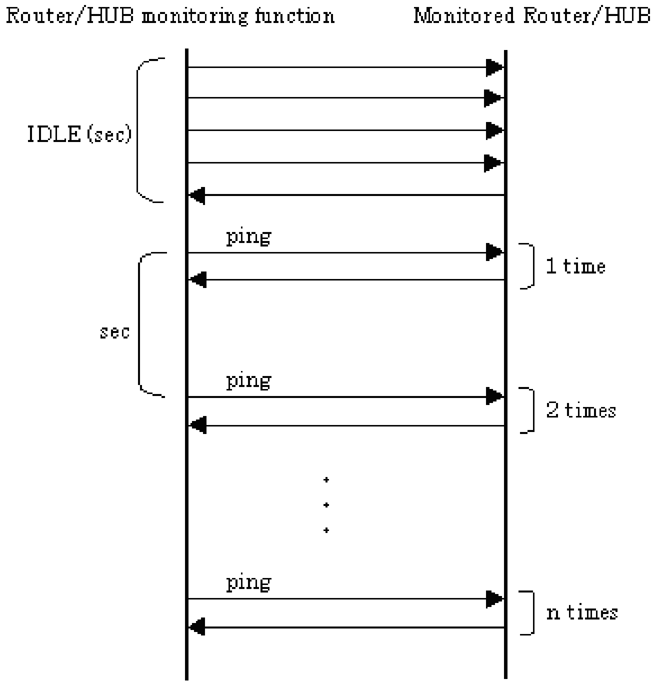


Figure 3.3 Basic sequence of Router/HUB monitoring

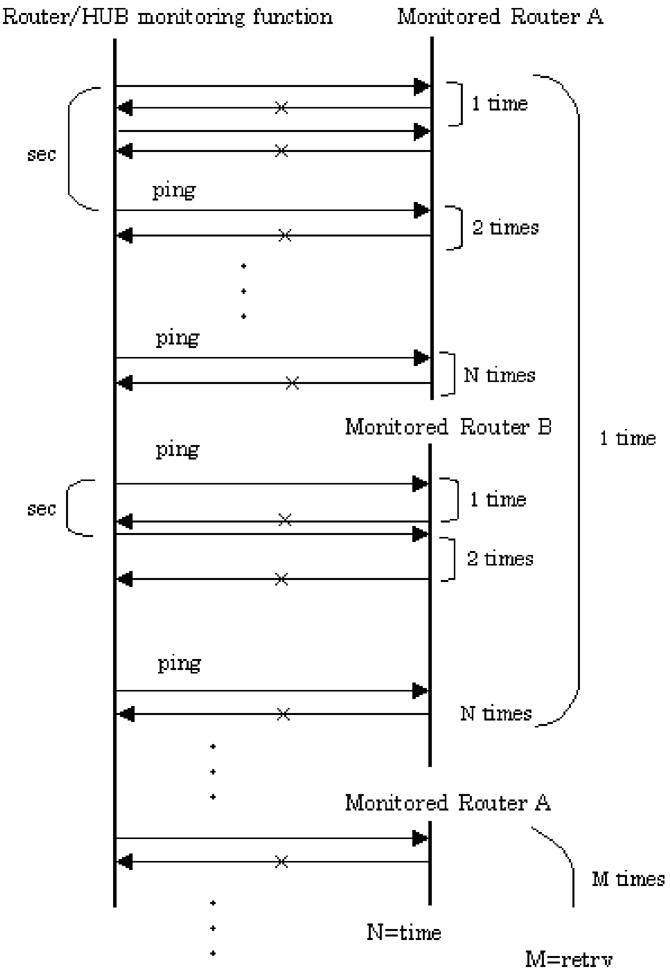


Figure 3.4 Router/HUB monitoring sequence after detect line fault

3.3.8.3 Setting operation history of interface up/down

Operation history of the interface up/down can be output as a syslog message. Since this message is output at the INFO level, the following setting is needed:

[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.

3.3.9 Setting communication party monitoring function

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.

3.3.10 Setting standby patrol function

3.3.10.1 Setting what to is be monitored

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.

3.3.10.2 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".

3.3.10.3 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".

3.3.11 Setting dynamic addition/deletion/switching function of real interfaces

3.3.11.1 Dynamic addition of real interfaces

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

3.3.11.2 Dynamic deletion of real interfaces

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

3.3.11.3 Dynamic switching of real interfaces

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

3.3.12 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 2.2.13, "User command execution function". In NIC switching mode, this function can be used to flush an ARP table, change the interface status, 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 party.

3.3.12.1 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, checking the communication (executes the ping command), and deleting the concerned information from the ARP table. 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 #
```

```
# 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
#
```

```
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.

[056-064]: Outputs a message that a command is executed, deletes the concerned ARP information after the interface is activated, and checks the 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
```

3.3.12.2 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.

3.3.13 Setting DR (Dynamic Reconfiguration)

3.3.13.1 Configure environment

To configure LAN environment of a Redundant Line Control Function using a DR linkage function, a configuration of "Figure 3.5 Recommended LAN configuration" is recommended.

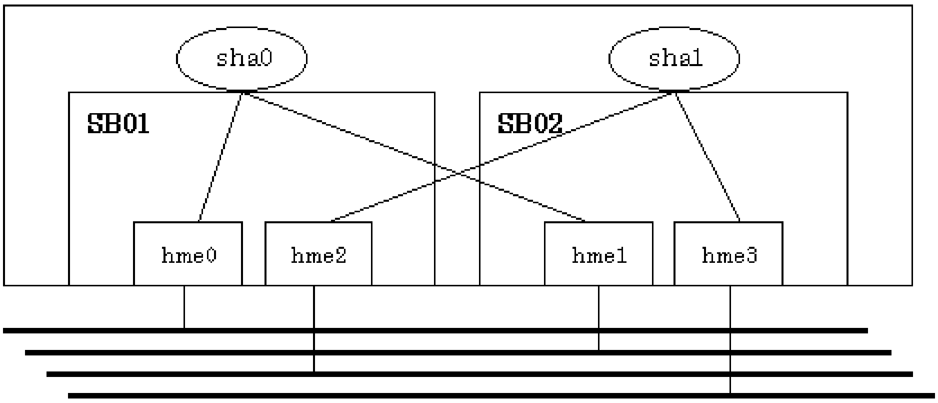


Figure 3.5 Recommended LAN configuration

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.

3.3.13.2 Workings when executing a DR command

(1) The workings when disconnected (a system board cut off)

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 linkage script of a Redundant Line Control Function.
When a virtual interface (sha0, etc.) of a single physical interface is defined and also a configured physical interface exists on the system board to be cut off, not possible to cut off a system board. A DR linkage 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) The workings when connected (a system board incorporated)

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 linkage script of a Redundant Line Control Function.

(3) The workings of cancellation

While executing a DR command, if decided to stop a process due to a certain reason, or to direct to stop a process to the inquiry, a system cancels execution of a DR command.
In a DR linkage script of a Redundant Line Control Function, it reconnects as a cancellation process of disconnection

and puts it back to the condition before disconnected.

{Notes}

- While exchanging SBs including a physical interface that configures a virtual interface of NIC switching mode (until it returns to the original state by "connect" after disconnected), a HUB monitoring function halts temporarily because it is not possible to switch NICs even if an error occurred in a transfer route. Then, it resumes automatically after exchanged SBs. Therefore, it is not possible to detect an error in a transfer route while exchanging SBs.
- After exchanged SBs including a physical interface that configures a virtual interface of NIC switching mode, monitoring of a transfer route starts without fail.

Chapter 4 Operation

This chapter explains how to operate Redundant Link Control Function.

4.1 Starting and Stopping Redundant Line Control Functio n

This section explains how to start and stop 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 polling function	Super user
	/opt/FJSVhanet/usr/sbin/hanetpoll off	Disabling the router polling function	Super user
Displaying the operation status	/opt/FJSVhanet/usr/sbin/dsphanet	Displaying the operation status of a virtual interface	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

4.1.1 Starting Redundant Line Control Function

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

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

4.1.2 Stopping Redundant Line Control Function

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

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

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.

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 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 party monitoring function.

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

4.5 Recovery Procedure from Line Failure

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

4.5.1 Recovery procedure from line failure in Fast switching mode

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

However, some applications may need to be restarted.

4.5.2 Recovery procedure from line failure in 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
```

4.5.3 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 4.5.1, "Recovery procedure from line failure in Fast switching mode" and 4.5.2, "Recovery procedure from line failure in RIP mode".

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

4.5.5 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.

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

How to recover when detected an error in a transfer route while exchanging SBs at the execution of DR is as follows. After recovered, execute drc -connect command and finish exchanging DRs.

[Fast switching mode]

See "4.5.1 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 "4.5.2 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 "4.5.3 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]

While exchanging SBs at the execution of DR, no error is detected in a transfer route because it halts a HUB monitoring function. It is not necessary to execute a recovery process in particular because it becomes possible to communicate after recovered a transfer route. Some applications may require to reactivate the application.

[GS/SURE linkage mode]

See "4.5.5 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 Backing up and Restoring Configuration Files

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

4.6.1 Backing up Configuration Files

Use the hanetbackup command to back up configuration files.

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

4.6.2 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 correct operation of Redundant Line Control Function cannot be assured if the system is not restarted.

Chapter 5 Operation on Cluster System

This chapter explains how to operate Redundant Line Control Function on cluster system.
Read the description of "cluster service" or "service" as "Cluster Application (userApplication)".

5.1 Outline of Cluster System Support

In cluster system, Redundant Line Control Function supports the following connection states:

- Active standby (1:1 and N:1)
- Mutual standby
- 1 node cluster

How cluster failover is dealt with in each mode is shown below. Only NIC switching mode supports SIS (Scalable Internet Services).

Mode	Cluster failover	SIS
Fast switching mode	Support	Not support
RIP mode	Not support	Not support
Fast switching/RIP mode	Not support	Not support
NIC switching mode	Support	Support
GS/SURE linkage mode	Not support	Not support

Only a logical IP address (takeover address) allocated to a virtual interface can be taken over. (No MAC addresses or system node names are taken over.) Physical interfaces used by the virtual interface cannot be set as objects of takeover (MAC address or IP address).

In this version, Redundant Line Control Function is not supporting making redundant transmission paths of PRIMECLUSTER Scalable Internet Services (SIS).

Figure 5.1 shows an example of address takeover in a virtual device.

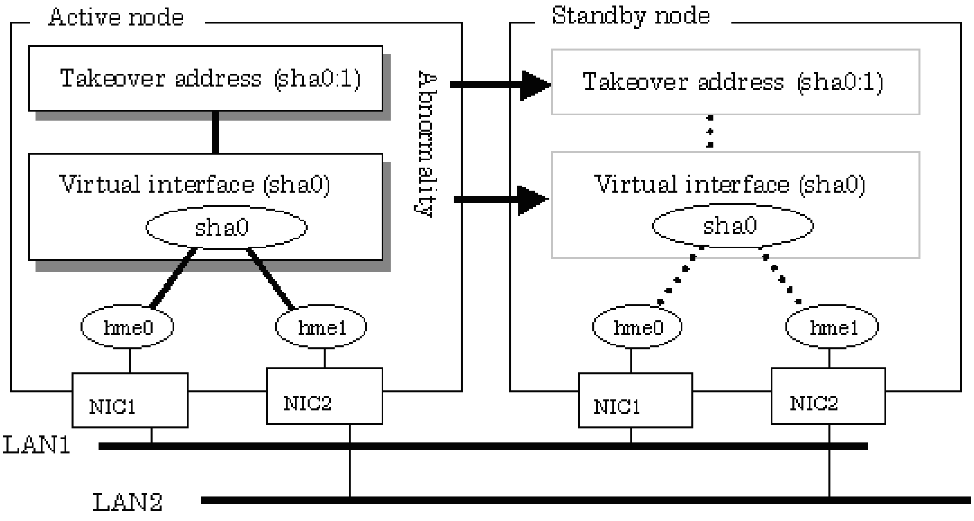


Figure 5.1 Address takeover

5.1.1 Active Standby

5.1.1.1 Switching operation

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

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

5.1.1.1.1 Switching operation in Fast switching mode

Figure 5.2 shows the active standby configuration diagram of duplicated operation in Fast switching mode. In the figure, the takeover virtual interface (sha0:65) is activated on active node A. If switching occurs due to a failure, the takeover virtual interface (sha0:65) is inactivated on active node A. Then, on standby node B, the takeover virtual interface (sha0:65) is activated on the already activated virtual interface (sha0). Thus, the virtual interface (sha0) on node A does not change statuses.

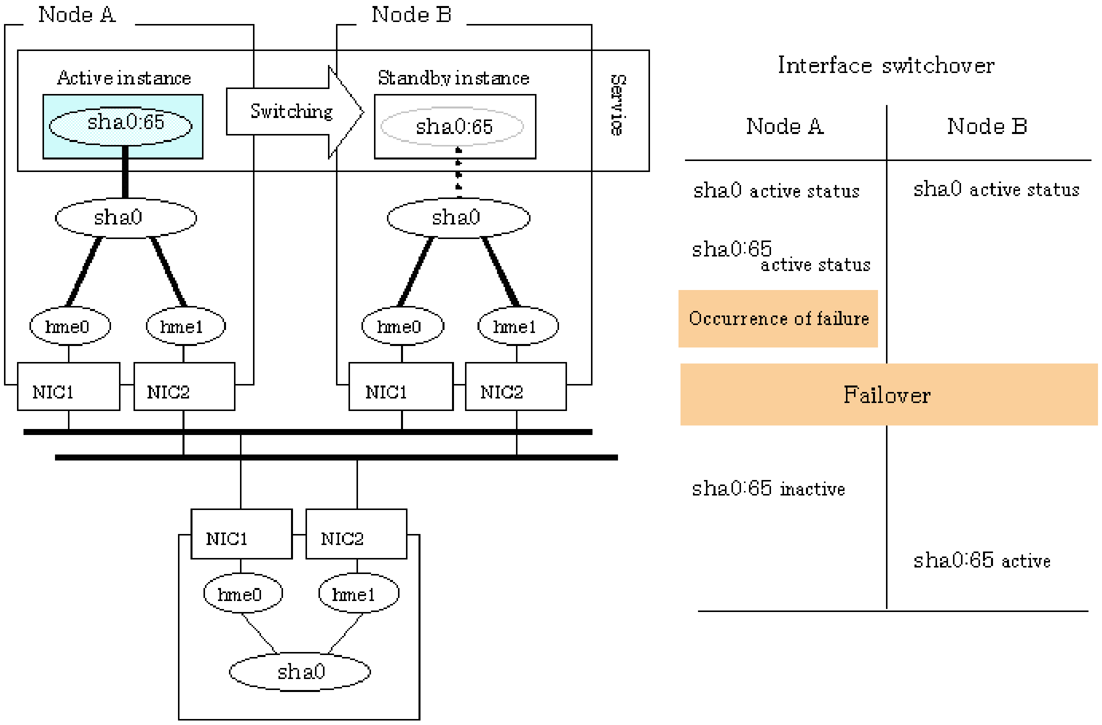


Figure 5.2 Standby configuration diagram of duplicated operation in Fast switching mode

5.1.1.1.2 Switching operation in 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 function
  Use the logical address takeover function to use a LAN in NIC switching mode both for jobs and management. In this case, communication is performed using a logical IP address for jobs and a physical IP address for management.
  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 cluster service.
  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 function I
  Use the physical IP address takeover function I to use a LAN in NIC switching mode both for jobs and management and specify only one IP address for one physical interface.
  As for the logical address takeover function, 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 cluster service. Thus, when clusters are switched, the TCP connection to the standby node is cleared. For the communication party device to make a connection again, the connection IP address must be changed.
- Physical IP address takeover function II
  Use the physical IP address takeover function II to use a LAN in NIC switching mode only for jobs. 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.

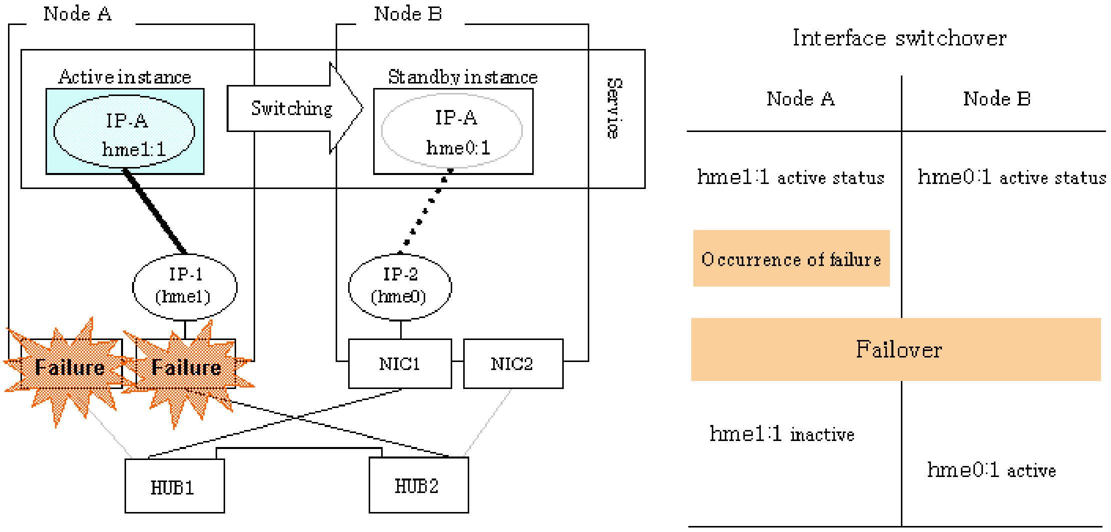


Figure 5.3 NIC switching mode (Logical IP address takeover function)

Figure 5.4 shows the active standby configuration diagram of duplicated operation in NIC switching mode (physical IP address takeover function I). (The physical IP address takeover function I activates a real NIC on the standby node.) The operation in this figure is as follows: On active node A, the takeover logical IP address (IP-A) is assigned the secondary interface (hme1) and activated. If switching occurs due to a failure, the already activated primary interface (hme0) on standby node B is first inactivated, assigned the takeover IP address (IP-A), and activated again. Then, on node A now in standby status, the secondary interface (hme1) that has been assigned the takeover IP address (IP-A) is assigned another IP address (IP-1) and activated again.

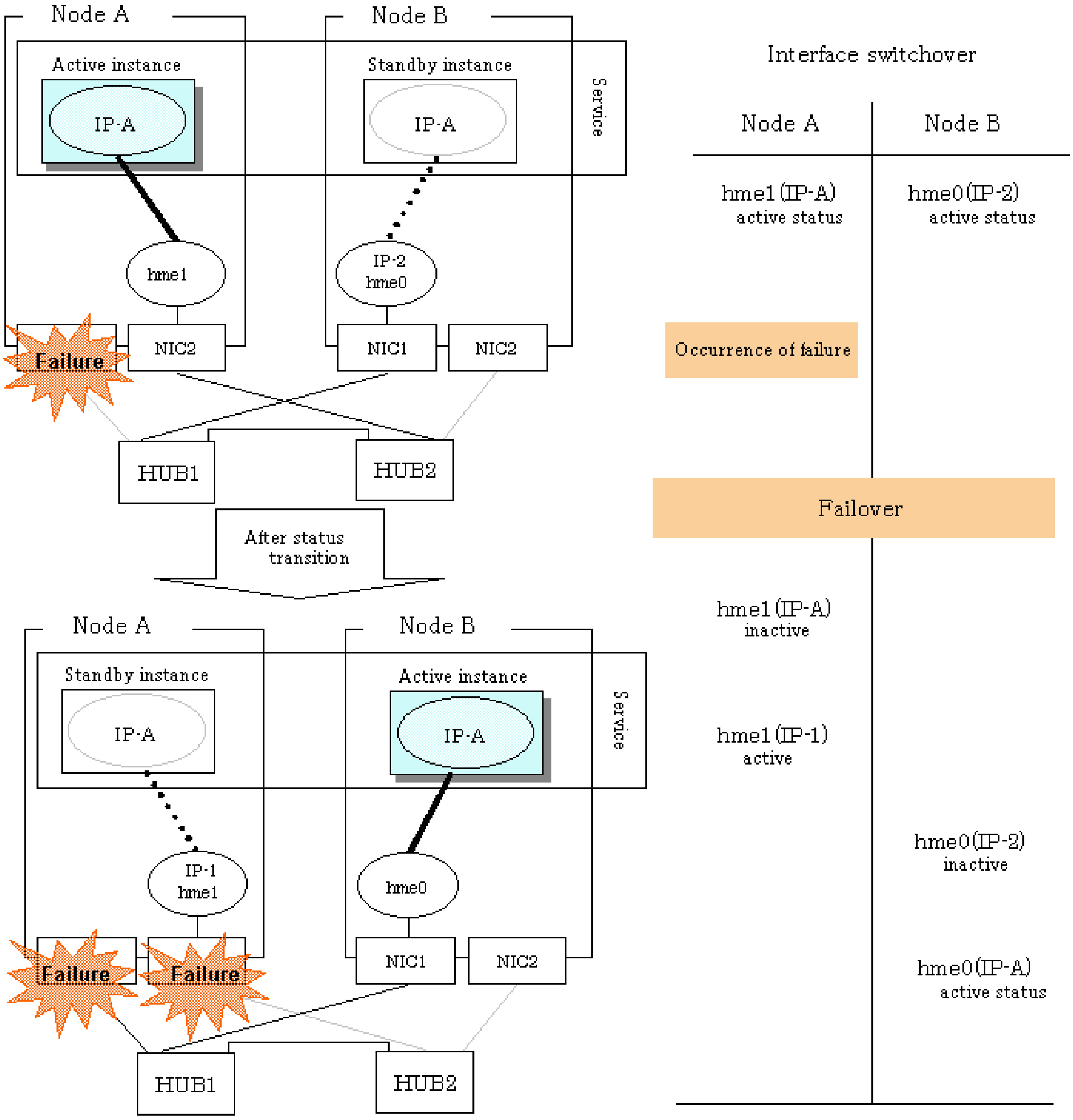


Figure 5.4 NIC switching mode (Physical IP address takeover function I)

Figure 5.5 shows the active standby configuration diagram of duplicated operation in NIC switching mode (physical IP address takeover function II). (The physical IP address takeover function II does not activate a real NIC on the standby node.) The operation in this figure is as follows: On active node A, the takeover virtual IP address (IP-A) is assigned the secondary interface (hme1) and activated. If switching occurs due to a failure, the already activated primary interface (hme0) on standby node B is assigned the takeover IP address (IP-A) and activated. Then, on node A now in standby status, the secondary interface (hme1) that has been assigned the takeover IP address (IP-A) is inactivated.

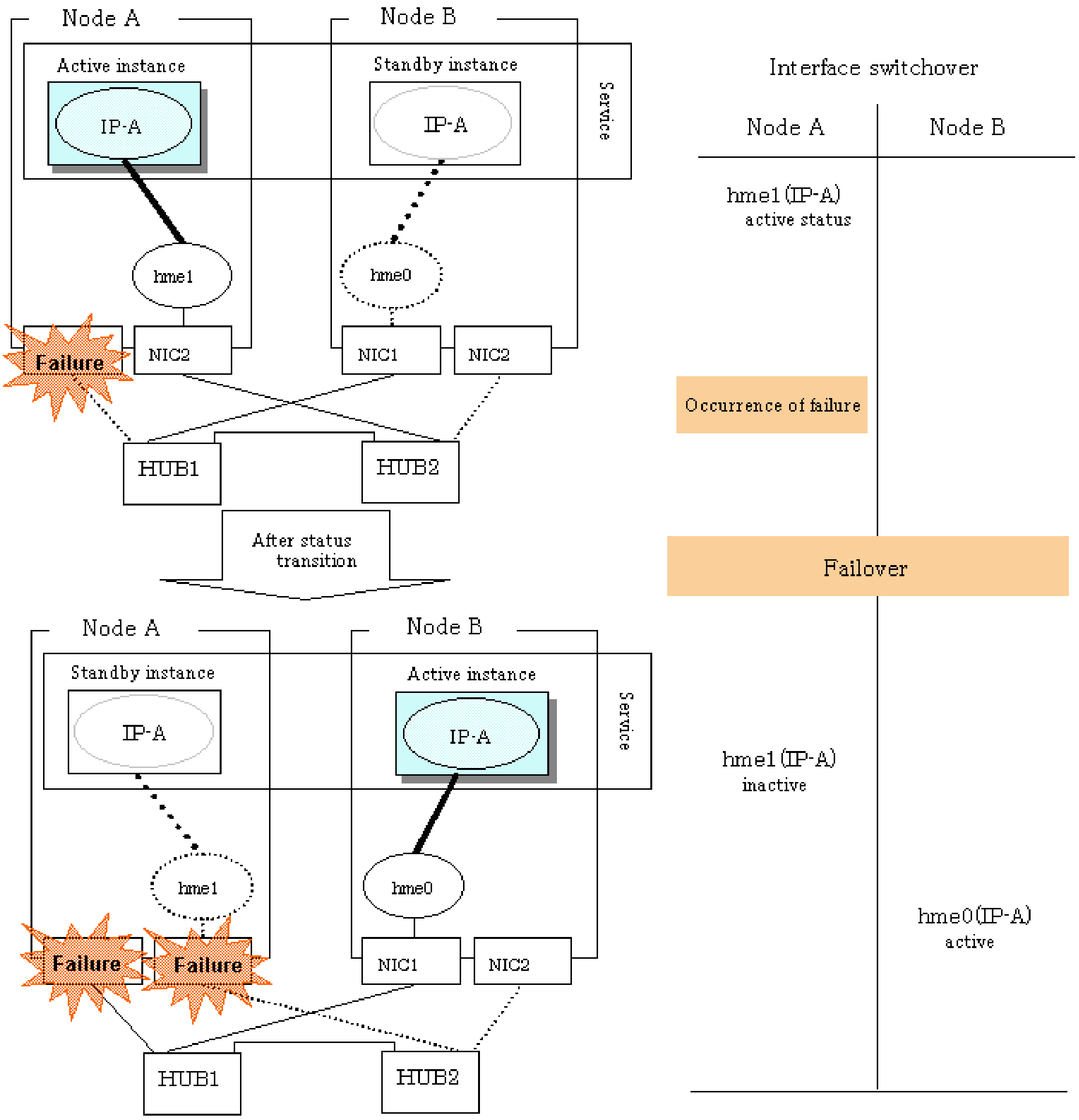


Figure 5.5 NIC switching mode (Physical IP address takeover function II)

5.1.1.2 Failback operation

The following shows a procedure of performing failback 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.

Using RMS, incorporate the node on which a failure has occurred into the concerned cluster service and restore the original operation status.

5.1.2 Mutual standby

5.1.2.1 Switching operation

Define more than one virtual interface and set the resources as separate services to enable mutual standby operation. During normal operation, the system communicates with the remote system using a virtual interface on the active instance of each service. If a failure (panic, hang-up, or line failure) occurs on the active instance, the standby instance takes over the virtual interface included in the active instance. Then, applications make reconnection to take over the communication from the active instance.

5.1.2.1.1 Switching operation in Fast switching mode

Figure 5.6 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, "Switching operation in Fast switching mode".

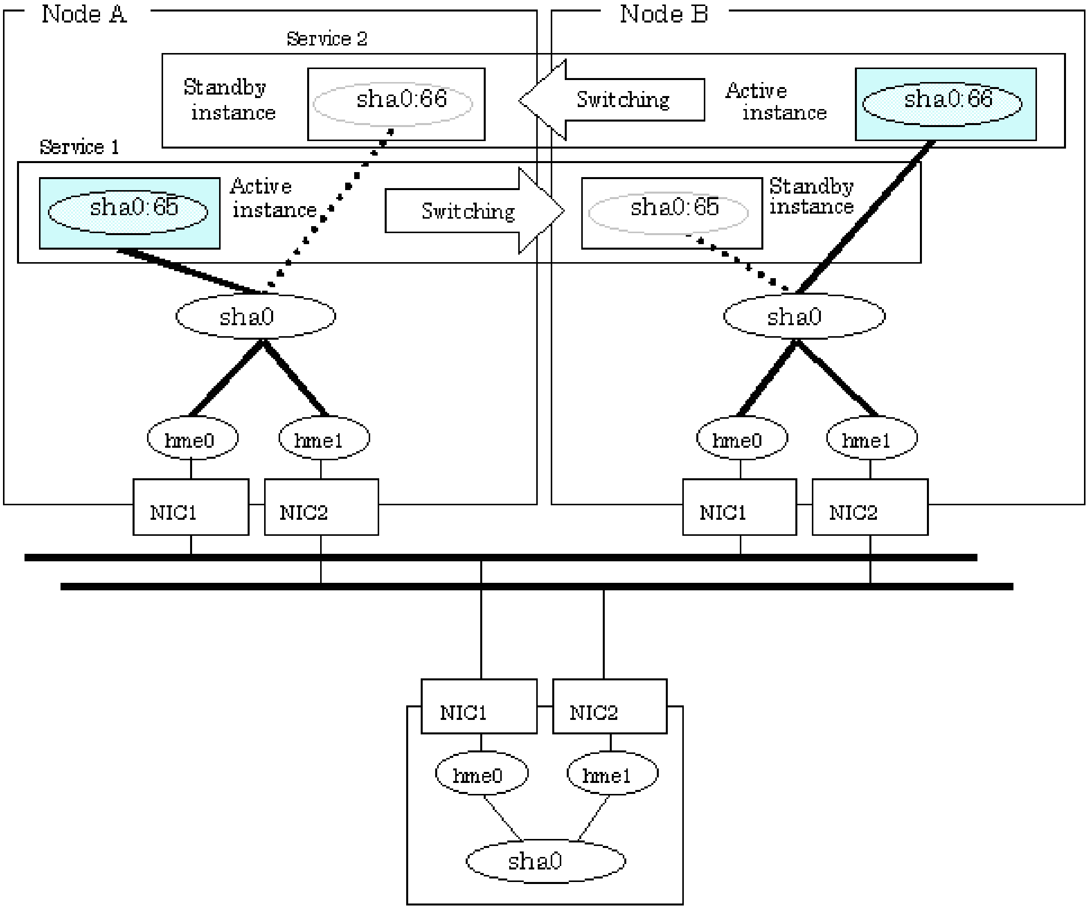


Figure 5.6 Mutual standby configuration diagram of duplicated operation in Fast switching mode

5.1.2.1.2 Switching operation in NIC switching mode

Figure 5.7 shows the mutual standby configuration diagram in NIC switching mode (without 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, "Switching operation in NIC switching mode".

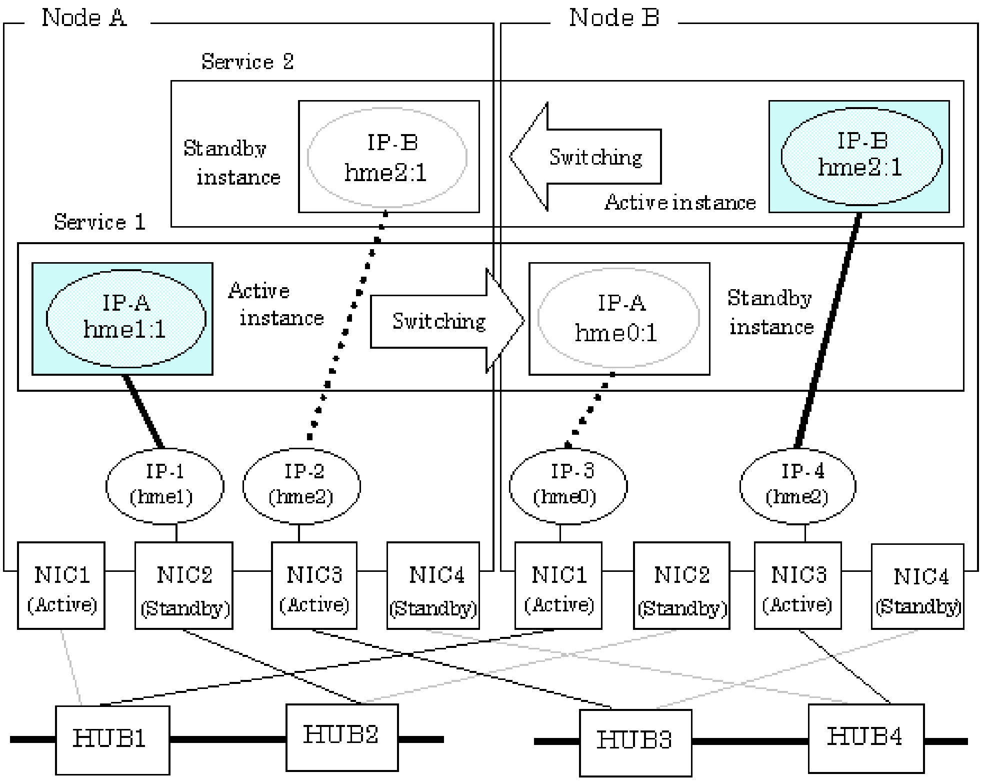


Figure 5.7 Mutual standby configuration diagram of duplicated operation in NIC switching mode (without NIC sharing)

Figure 5.8 shows the mutual standby configuration diagram in NIC switching mode (with 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, "Switching operation in NIC switching mode".

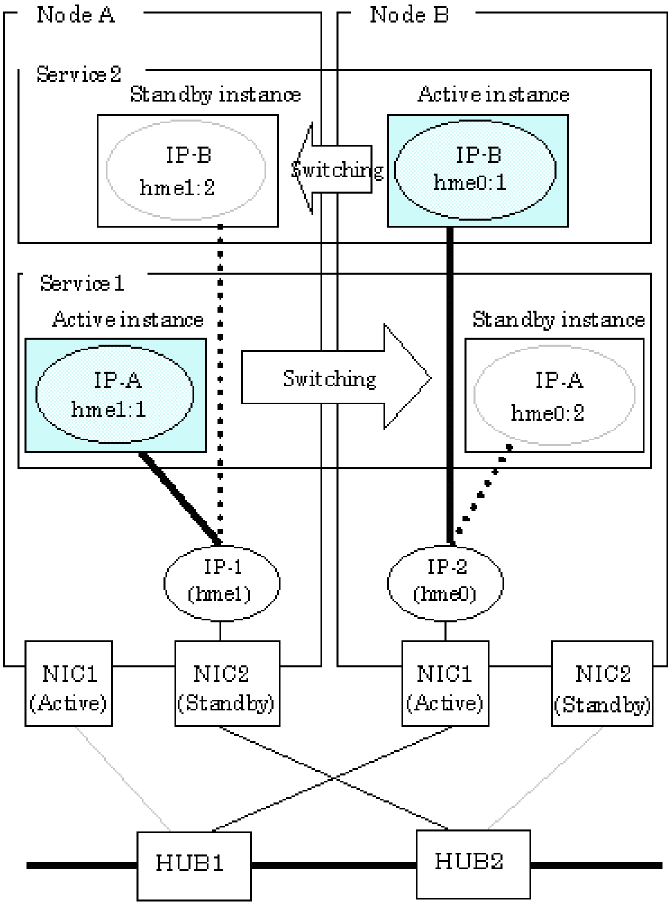


Figure 5.8 Mutual standby configuration diagram of duplicated operation in NIC switching mode (with NIC sharing)

5.1.2.2 Failback operation

The failback is performed in the same way as for the active standby configuration. For information, see Section 5.1.1.2, "Failback operation".

5.2 Adding configuration for Cluster System

In a Redundant Line Control Function, it is necessary to set the configuration information as well as an ordinary environment, and also to register the resources. Figure 5.9 shows a flow of the procedure to add a cluster environment definition. In the mutual standby operation, repeat "5) Setting of a Wizard" of the following procedure "1) Setting of the configuration information". (Execute "Reactivation of the system" in each node at last only once after finished all the setting.) See "Appendix B Example of environment setting" for an example of the setting.

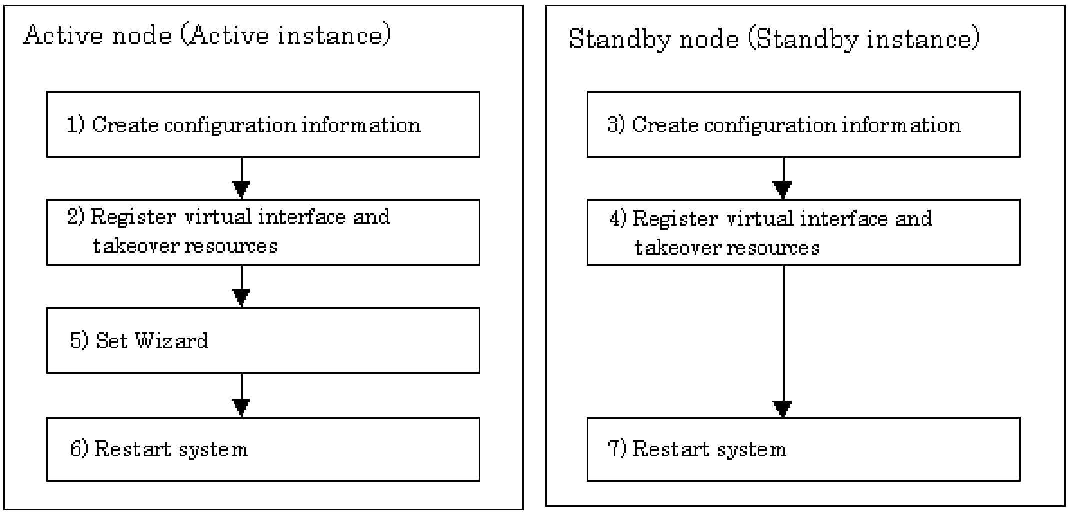

Active node (Active instance)
1) Create configuration information
2) Register virtual interface and takeover resources
5) Set Wizard
6) Restart system
Standby node (Standby instance)
3) Create configuration information
4) Register virtual interface and takeover resources
7) Restart system

Figure 5.9 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 5.1 lists the cluster definition operation commands.

Table 5.1 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, "Installation."

5.2.2 Registration of a virtual interface and the takeover resources

Register the resources for a virtual interface. It is necessary to set this in a node of both systems. When setting for Fast switching mode, it is necessary to set a "-i 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.

[Virtual interface and takeover resource registration]

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n "virtual-interface-name" [-i
takeover-IP-address]
```

5.2.3 Setting by a Wizard

Set a node to configure a cluster configuration using a virtual interface and the takeover resources. Set this in a node either of the active node or the standby node. See "The sub application Gls" for the detail.

5.2.4 Restarting the system

Restart the systems on both nodes.

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

This section explains the procedure to delete and how to delete a cluster environment definition of the Redundant Line Control Function. Figure 5.14 shows a flow of the procedure to delete a cluster environment. In the mutual standby operation, repeat "5) Deletion of a virtual interface and the takeover resources" of the following "2) Deletion of a Wizard definition".

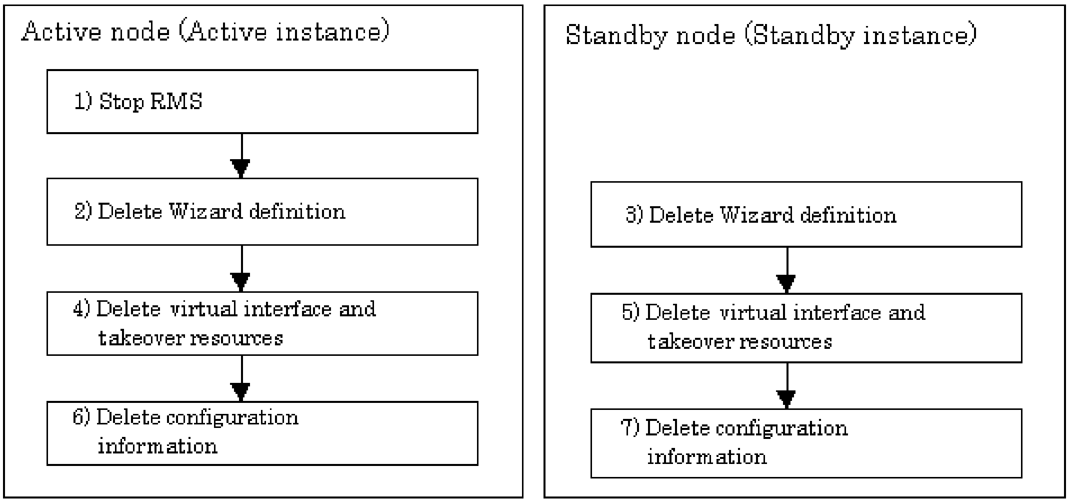

Active node (Active instance)
1) Stop RMS
2) Delete Wizard definition
4) Delete virtual interface and takeover resources
6) Delete configuration information
Standby node (Standby instance)
3) Delete Wizard definition
5) Delete virtual interface and takeover resources
7) Delete configuration information

Figure 5.10 Flowchart for deleting configuration for cluster system

5.4.1 Stopping RMS

Stop RMS. See "RMS Configuration and Administration" for the detail.

5.4.2 Deletion of a Wizard definition

Delete the node information to configure a cluster configuration using a virtual interface and the takeover resources. Be sure to set this in both nodes. See "The sub application Gls" for the detail.

5.4.3 Deletion of a virtual interface and the takeover resources

Delete a virtual interface to control a cluster from the resources database. Set this in a node of the active node and the standby node. An example of deletion is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n
"logical-virtual-interface-name"
```

5.4.4 Deletion of a Configuration information

Delete the configuration information set to construct the virtual interface. It is necessary to delete the configuration information on both nodes of the active node and the standby node. See "3.2.3 Deleting configuration information" for the deletion of configuration information.

Chapter 6 Maintenance

This chapter explains commands and other helpful tools (including parameters) that collect troubleshooting information in the event of a problem in Redundant Line Control Function.

6.1 Redundant Line Control Function Troubleshooting Dat a 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.

[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:

Type	Collected information	File name when collected
Network information	uname -a ifconfig -a netstat -na netstat -ni netstat -nr netstat -np ndd -get /dev/ip ip_forwarding ipcs -a ls -l /etc/defaultrouter ls -l /etc/notrouter ls -l /etc/hostname* /etc/hosts /etc/netmasks /etc/nsswitch.conf	Uname_a ifconfig_a netstat (") (") (") ip_forward ipcs_a filelist_etc (") (") etc/hosts etc/netmasks etc/nsswitch.conf
Process information (Not collected when collecting minimum.)	ps -ef pstack (Daemon only or all) /var/adm/messages*	ps_ef pstack var/adm/messages*
Information of a Redundant Line Control Function	hanetconfig version patchadd -p | grep hanet dsphanet dsphanet -o dsphanet -c dsppoll dsppoll -c /etc/opt/FJSVhanet/config/* /var/opt/FJSVhanet/log/* ls -la /var/opt/FJSVhanet/tmp	version patchinfo dsphanet (") (") dsppoll (") etc/opt/FJSVhanet/config/* var/opt/FJSVhanet/log/* filelist_tmp
Cluster information (Not collected when collecting minimum.)	/usr/opt/reliant/bin/hvdisp -a /var/opt/reliant/log/*	hvdisp_a var/opt/reliant/log/*

[Output form]

The collected materials are compressed and stored by tar and compress commands. A stored file name is "machine name" + "Date collected (YYMMDDhhmm)".tar.Z.

Ex.) hostname0205311538.tar.Z

When decompressed the compressed collected materials, they are deployed in the following directory configuration:

```
/Optional_directory/hanetinfo/config/* (Under /etc/opt/FJSVhanet/config)
```

```
                     /log/* (Under/etc/opt/FJSVhanet/log)
                     /version
                     /patchinfo
                     /dsphanet
                     /dsppoll
                     /filelist_tmp
/Optional_directory/RCInfo/log/* (Under /var/opt/reliant/log)
                   /hvdisp_a
/Optional_directory/OSInfo/etc/hosts
                       /netmask
                       /nsswitch.conf
/Optional_directory/OSInfo/adm/messages*
                   /uname_a
                   /ifconfig_a
                   /netstat
                   /filelist_etc
                   /ip_forward
                   /ipcs_a
                   /ps_ef
                   /pstack
```

[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 References

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

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	Super 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

```
/opt/FJSVhanet/usr/sbin/hanetconfig create [inet | inet6] -n devicename
       -m {t|r|b|n|c|d|e|p|q} [-i ipaddress1[/prefix]] [-e ipaddress2]
       -t interface1[,interface2,.....] [-a MAC-address]
```

- When creating a logical virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -i ipaddress
```

[inet | inet6]

Specify an IP address form to set to a virtual interface.

inet : IPv4 address
inet6 : IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of "create") before other options.
This opetion is valid only in NIC switching mode (a logical IP address takeover function) (the operation mode is "d").

-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.

-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 (real interface definition)
Specify this parameter to use the Redundant Line Control Function in GS/SURE linkage mode. A real 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 real 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. Communication is performed by activating a physical interface to be used and its logical interface and taking over the IP address attached to the logical interface.

e: NIC switching mode (physical IP address takeover function)
Specify this parameter to use the Redundant Line Control Function in NIC switching mode. Communication is performed by taking over the IP address attached to the real interface without activating a logical 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'	Not support	O	O	X	X	O (*1)
'r'	Not support	O	O	X	X	O (*1)
'b'	Not support	O	O	X	X	O (*1)
'n'	Not support	O	O	X	X	O (*4)
'c'	Not support	O	O	X	X	O (*5)
'd'	Support	O	O	O (*6)	X	O (*2)
'e'	Not support	O	O	O (*7)	X	O (*2)
'p'	Not support	O	X	X	O	O (*3)
'q'	Not support	O	X	X	O	O (*3)

Explanation of symbols) 0: Required, X: Not required

*1 Specify a real interface (The same real interface can be specified if the operation mode is "t", "r", or "b").
*2 Specify a real interface that is not specified in any other operation mode.
*3 Specify a virtual interface specified in the operation mode "d" or "e".
*4 Specify one real interface that is not specified in any other operation mode.
*5 Specify a virtual interface created in operation mode "n".
*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).

-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 (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 file. It is possible to specify this option only when specified inet for an address form. (When specified inet6, a link local address is automatically assigned.) It is necessary to set this option in NIC switching mode (operation mode is "d" or "e"). In cluster operation, it is possible to omit this option if an interface of NIC switching mode (operation mode is "e") is not activated by a standby node.

-t interface1,interface2,...:

Specify interface names to be bundled by a virtual interface, by listing them delimited with a comma (,).

Specify virtual interface names (such as sha1 and sha2) for GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

Specify real interface names (such as le0 and hme0) for any other mode or function than GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

-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.

The following is the command format for building a logical virtual interface.

A logical virtual interface can be set only in operation modes "r", "t" and "b".

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -i ipaddress
```

-n devicename:

Specify the name of a logical virtual interface for which the configuration information should be set. Specify the logical virtual interface name with a string that begins with "sha" and is followed by a value (0 to 255), a delimiting colon (:), and another value (2 to 64) (such as sha0:2 and sha1:10). If you specify a logical virtual interface in any other format, an error message is output and this command terminates abnormally.

-i ipaddress:

Specify a host name or IP address to be attached to a logical virtual interface specified in the -n parameter. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts file. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation. When you specify address information for a logical virtual interface, be sure to specify an address in the same subnet as the address of a corresponding virtual interface. Communication may be disabled if any other subnet is specified.

(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 real 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. 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

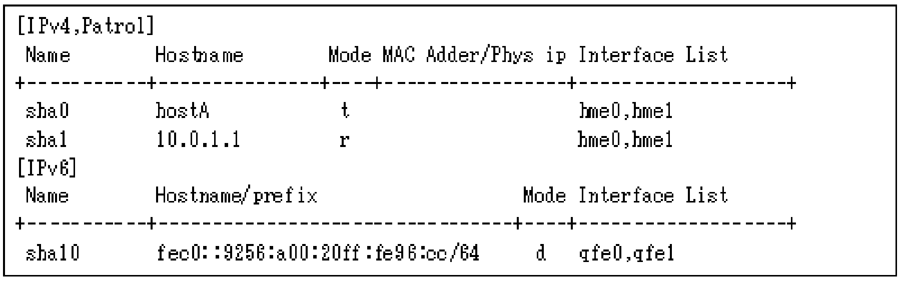
Use the print command to display the current configuration information. The following is the format of the print command.

```
/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
[IPv6]
 Name       Hostname/prefix                 Mode Interface List
+-----------+--------------------------------+----+-------------------+
 sha10      fec0::9256:a00:20ff:fe96:cc/64     d   qfe0,qfe1
```

[IPv4,Patrol] : The information of an IPv4 virtual interface and standby 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.

MAC Adder/Phys ip : Outputs a MAC address defined in standby patrol mode.

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

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

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify [inet | inet6] -n devicename
            {[-m t|r|b]|[-i ipaddress1[/prefix]]|[-e ipaddress2]|
            [-t interface1[,interface2.....]]|[-a MAC-address]}
```

- When changing configuration information of a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename -i ipaddress
```

[inet | inet6]

Specify an IP address form to set to a changing virtual interface.

inet : IPv4 address
inet6 : IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of modify) before other options.

-n devicename:

Specify the name of a 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:

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 file. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation. When you specify address information for a logical virtual interface, be sure to specify an address in the same subnet as the address of a corresponding virtual interface. Communication may be disabled if any other subnet is specified.

-e ipaddress2:

Specify an IP address to be attached to a real interface. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts file. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation.

This parameter can be modified only if the operation mode of a virtual interface to be modified is NIC switching mode (operation mode "d" or "e").

-t interface1,interface2,...:

Specify interface names to be bundled by a virtual interface, by listing them delimited with a comma (,).

Specify virtual interface names (such as sha1 and sha2) if the operation mode of a virtual interface to be modified is GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

Specify real 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:

Specify a local MAC address as 02:XX:XX:XX:XX:XX (X represents a hexadecimal from 0 to F).

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").

The following is the command format of the modify command that modifies the configuration information of a logical virtual interface.

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename -i ipaddress
```

-n devicename:

Specify the name of a logical virtual interface whose configuration information should be modified (such as sha0:2 and sha1:10).

-i ipaddress:

Specify a host name or IP address to be attached to a logical virtual interface. When you specify address information for a logical virtual interface to be modified, 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.

(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 -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 is valid only in NIC switching mode (a logical IP address takeover function) (operation mode is "d").

-n devicename1,devicename2*:

Specify the names of virtual interfaces (such as sha0 and sha1) or logical virtual interfaces (such as sha0:2 and sha1:10) whose configuration information should be deleted.

all:

Specify this parameter to delete all the defined virtual and logical interfaces.

(6) version command

The version command displays the version of the hanetconfig command. 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 2.4
```

[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 real 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.
- Only an option that can be set can be modified.
- 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 real 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.
- 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, not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts file. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control Function to use the corresponding host name and to set the definition again.
- When 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.

[Examples]

Execution example 1

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
```

Execution example 2

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
```

Execution example 3

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
```

Execution example 4

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
```

Execution example 5

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 r -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
```

Execution example 6

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 r -i hosti -t hme0
```

Execution example 7

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 02:00:00:00:00:00
-t sha0
```

Execution example 8

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 -e hostj
-t hme0,hme1

# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01
-t sha0
```

Execution example 9

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 real 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 sha0 -m n -i hostd -t hme0

# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i hoste -t hme1

# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m c -i hostf -t sha0,sha1
```

Execution example 10

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
```

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. If -n option is not specified, this command activates all virtual interfaces and logical virtual interfaces that have been set. By specifying -n option, specific virtual interfaces can be activated.

[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 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, "Installation".
- 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").

- Virtual interfaces in GS/SURE linkage mode (operation mode "n") are automatically activated when a virtual interface that bundles these virtual interfaces is activated.
- 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"). Not possible to specify to a virtual interface of GS/SURE linkage 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.

[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 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. When not specified the -n option, strhanet command makes it possible to deactivate all the virtual interfaces. By specifying the -n option, it is possible to deactivate a specific virtual interface only.

[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 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.
- 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"). 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.
- When deactivating a virtual interface, if stacked physical interfaces are not used at all, deactivate them as well.

[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 activate all virtual interfaces of 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. If the -n option is not specified, this command displays the statuses of all virtual interfaces that are properly defined. Specify the -n option to display the statuses of only specific 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

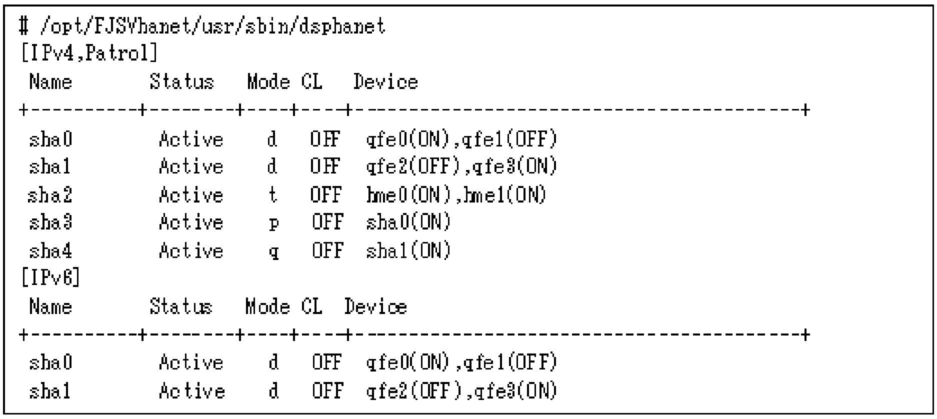
Displays all communication parties of virtual interfaces defined in Fast switching mode (operation mode "t"). This option does not display communication parties of virtual interfaces not yet activated using the strhanet command.

-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 party 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)
```

[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.

Active	: Active status
Inactive	: Inactive status

Mode Outputs the operation mode of a virtual interface.

t: Fast switching mode
r: RIP mode
b: Fast switching/RIP mode
n: GS/SURE linkage mode (real 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)

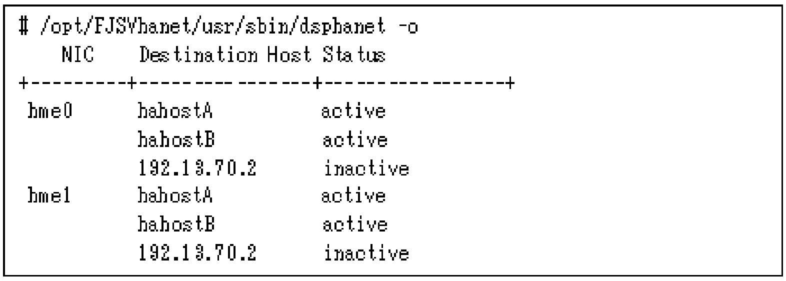
CL : Cluster definition status

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.

ON : Enabled
OFF : Disabled
STOP : Ready for use
FAIL : Error in one system
CUT : Unused

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
          192.13.70.2     inactive
 hme1     hahostA         active
          hahostB         active
          192.13.70.2     inactive
```

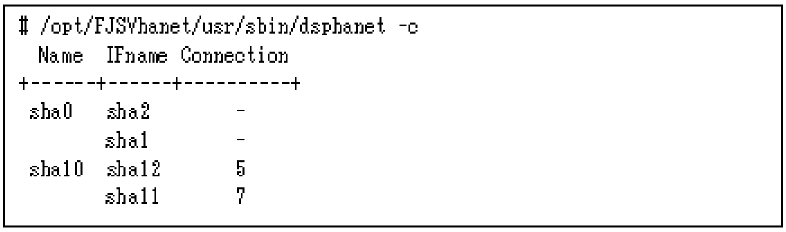
NIC : Outputs a real interface name.

Destination Host : Outputs the host name or IP address of the communication party.

Status : Outputs the status of the communication party.

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
```

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 party 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 party. This enables the system to continue communication using other communication paths when a failure occurs. Use the create command to generate a communication party. The following is the command format for generating a monitoring destination:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddr
    -t nicaddr1[:pm-id][,nicaddr2[:pm-id],...] -m { on | off }
    [-r { on | off }] |
    -i ipaddr -c client1[:subnet][,client2[:subnet],...]
```

-n node:

Specify a name by which to identify the node of a communication party, using up to 16 one-byte characters.

-i ipaddress:

Specify a host name or IP address of a virtual interface held by the communication party. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts file. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation.

-t nicaddr1[: pm-id][, nicaddr2[: pm-id],...]:

Specify the host names or IP addresses of real interfaces bundled by a virtual interface, by listing them delimited with a comma (,).

nicaddrX:

Specify the host name or IP address of a real interface bundled by a virtual interface.

pm-id:

Specify the identifier of the PM (processor module) group to which the real interface of the communication party belongs when it is the SURE system. Specify a number from 1 to 8. This option is not required if the communication party 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 party 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 party.

off:

The local host does not monitor the communication party.

-r on | off:

Sets if or not a RIP packet is sent from the other device. 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 client1[: subnet][, client2[: subnet], ...]:

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 (,).

clientX:

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 file. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation. If a remote network is specified, a "subnet" must be specified.

subnet:

This option must be specified when a remote network is specified in "clientX". 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]
```

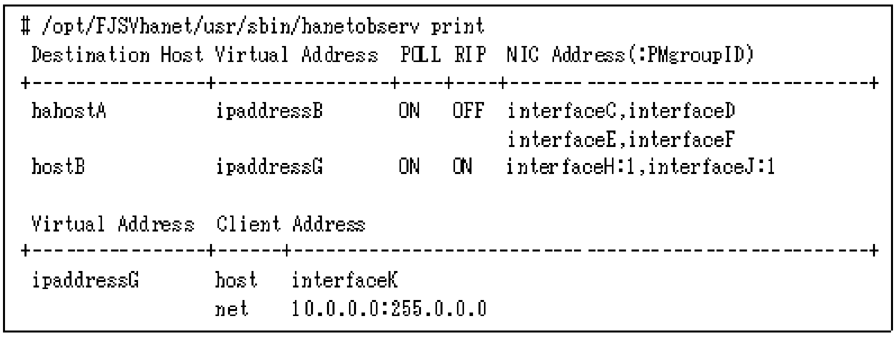
-o:

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  interfaceC,interfaceD
                                             interfaceE,interfaceF
 hostB            ipaddressG       ON   ON   interfaceH:1,interfaceJ:1

 Virtual Address  Client Address
+----------------+------+------------------------------------------------------+
 ipaddressG       host   interfaceK
                  net    10.0.0.0:255.0.0.0
```

* The first real interface names in the real interface name list are interfaceC, interfaceE, and interfaceH in the above example.

Destination Host : Outputs the host name of the communication party.

Virtual Address : Outputs the virtual interface name.

POLL : Outputs the monitoring mode.

ON : The local host monitors the communication party.
OFF : The local host does not monitor the communication party.

RIP : With or without an RIP packet sent from the other end device.

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 real interface names bundled by a virtual interface. An ID value is shown in parentheses.

Virtual Address : Outputs the virtual interface name.

Client : Outputs the network type of the communication destination.

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 interface,new-interface1[:pm-id][,new-interface2[:pm-id],...] |
   -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 interface, new-interface1[: pm-id][, new-interface2[: pm-id], ...]:

Specify the names of real 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.

interface:

Specify the first real interface names in the real interface name list that bundles real interface names that are set in the monitoring destination information (to be modified). Check the first real interface names using the print command of hanetobserv.

new-interface1[: pm-id][, new-interface2[: pm-id], ...]:

Specify all the real interface names 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-interfaceX:

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 real interface of the communication party belongs when it is the SURE system. Specify a number from 1 to 8. This option is not required if the communication party is GS.

-m on | off:

Specify the operation mode of the monitoring destination 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 real interfaces bundled by a virtual interface is modified.

-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 ipaddr1[,ipaddr2,...] |
                -n node -i ipaddress
    -t nicaddr1[:pm_id][,nicaddr2[:pm_id],...] |
    -c all |
    -i ipaddr -c all |
    [-i ipaddr] -c client1[:subnet][,client2[:subnet],...]
```

-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 ipaddr1[, ipaddr2, ...]:

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 nicaddr1[: pm_id][, nicaddr2[: pm_id], ...]:

Delete the real interface list under the virtual interface. Specify the first real interface name under the virtual interface to be deleted. You can specify more than one real interface name lists by listing them delimited with a comma.

If only one real interface name list is defined under the virtual interface, the virtual interface is also deleted. If only one virtual interface is defined under node, the definition information including the virtual interface is deleted. Check the first real interface name using the print command of hanetobserv.

-c all

Delete the definition that is set to use the TCP relay function.

-i ipaddr -c all

Delete all the information under the virtual interface information specified in the "-i" option.

[-i ipaddr] -c client[: subnet][, client2[: subnet], ...]

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 party monitoring function is set or changed must be defined in /etc/inet/hosts.
- The node name information must not be specified as "all".
- Up to 32 real interfaces can be specified to be bundled by the virtual interface of the communication party 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, not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts file. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control Function to use the corresponding host name and to set the definition again.

[Examples]

(1) create command

The following shows a setting example in which monitoring is performed while the communication party's node hahostA has virtual interface vip1, which bundles two real interfaces interfaceC and interfaceD. 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 interfaceC,interfaceD -m on
```

The following shows a setting example in which monitoring is not required because the already defined communication party hahostA has virtual interface vip2, which bundles real interfaces interfaceF and interfaceG. 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 interfaceF,interfaceG -m off
```

The already defined communication party hahostA has virtual interface vip2, which bundles two real interfaces interfaceF and interfaceG. The following shows a setting example in which new real interfaces interfaceH and interfaceJ are bundled and added to virtual interface vip2. The system takes over the monitoring mode used when real interfaces interfaceF and G 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 interfaceH,interfaceJ
```

Define the SURE interface to be used to communicate with the node of the communication party when the TCP relay function in GS/SURE linkage mode is used. The SURE virtual interface (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 party. 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 party monitoring destination information to hahostH.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB,hahostH
```

The following shows an example of changing the virtual interface name (vip1) of the node (hahostB) in the communication party monitoring destination information to vip2.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip1,vip2
```

The following shows an example of changing the real interface names (interface1 and interface2) bundled by virtual interface (vip1) of the node (hahostB) in the communication party monitoring destination information to interface3, interface4, and interface5.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip1
              -t interface1,interface3,interface4,interface5
```

The following shows an example of changing the real interface names (interface6 and interface7) bundled by virtual interface (vip2) of the node (hahostB) in the communication party monitoring destination information to interface7 and interface8.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip2
              -t interface6,interface7,interface8
```

The following shows an example of changing the "on" setting of the monitoring mode of the node (hahostB) in the communication party monitoring destination information to "off".

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -m off
```

The following shows an example of changing the communication party (interface6) in the relay destination information (interface6 and interface7) of the virtual interface (vip2) in the communication party 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,interface7
```

(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 interface (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 interface (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 real interface name list (interfaceC, interfaceD) under the virtual interface (vip1) in the TCP relay information.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -i vip1 -c
interfacecC,interfacecD
```

7.6 hanetparam Command

[Name]

hanetparam - Setting up the monitoring function when Fast switching mode, NIC switching mode, or the standby patrol function is used

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetparam -w | -m | -l | -p | -o | -t | -d | -c value
/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 party 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 party 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. By default, cluster failover is specified to be performed if communication fails five consecutive times. This parameter is enabled only for Fast switching mode.

-t value

Use this parameter to change the activation timing of a virtual interface in Fast switching mode registered in the cluster resources. Specify "initialize" or "init" in value to activate the relevant virtual interface when the system is started up. This procedure allows "INTERSTAGE Traffic Director", etc. to be used as the host application. Alternatively, specify "cluster" in value to activate the relevant virtual interface according to an instruction from the cluster management daemon when the system is started up. Initially, "cluster" is specified in value. This parameter is enabled only for Fast switching mode.

-c value

When operating Fast switching mode on a cluster system and when an error occurred in all transfer routes at the activation of a service, 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 service.
Specify "off" to value for not executing failover between clusters when an error occurred in all transfer routes at activation of a service.
"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 party 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

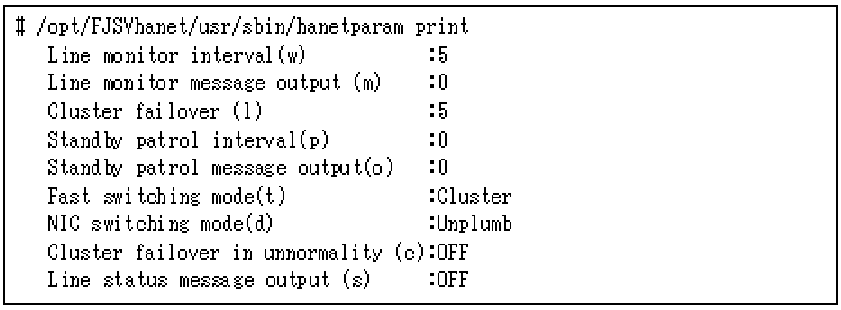
Use this parameter to change the method of inactivating the standby interface in NIC switching mode. Specify "plumb" in value to inactivate the standby interface and set "0.0.0.0" as the IP address. This procedure allows "INTERSTAGE Traffic Director", etc. to be used as the host application. Alternatively, specify "unplumb" in value to inactivate and delete the standby interface. Initially, "unplumb" is specified in value. This parameter is enabled only for NIC switching mode.

< 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)        :0
   Standby patrol message output(o)  :0
   Fast switching mode(t)            :Cluster
   NIC switching mode(d)             :Unplumb
   Cluster failover in unnormality (c):OFF
   Line status message output (s)    :OFF
```

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.

Fast switching mode (t) : Outputs the timing of activating Fast switching mode registered in the cluster resources.

- Cluster : Activates the virtual interface according to an activation instruction from the cluster service.
- Initialize : Activates the virtual interface when the system is initialized.

NIC switching mode (d) : Outputs the method of inactivating the standby interface in NIC switching mode.

- 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 cluster service.

- ON : Cluster switching immediately occurs.
- OFF : Cluster switching does not occur at activating a service.

Line status message output (s) : With or without a message output when a physical interface changed the status.

- 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.

[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 party 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 party fails five consecutive times.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -l 5
```

(4) Example of setting the activation timing in Fast switching mode registered in the cluster resources
The following shows an example of using this command to activate the virtual interface when the system is initialized (using "INTERSTAGE Traffic Director", etc. as the host application).

```
# /opt/FJSVhanet/usr/sbin/hanetparam -t initialize
```

(5) A setting example of the workings when an error occurred in every transfer route at the activation of a service
An example of a command to execute failover between clusters when an error occurred in every transfer route immediately after activated a cluster service is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanetparam -c on
```

(6) 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 party 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", 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	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
polladdr1[,polladd2 [-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 polladdr1[,polladdr2]:

Specify a monitor-to host name or IP address. Specify a monitor-to host name or IP address to "polladdr1" when activating a Primary interface. Specify a monitor-to host name or IP address to "polladdr2" 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 "polladdr2". 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 the copy command to create copy monitoring destination information on a virtual interface in NIC switching mode. This command thus allows monitoring destination information to be automatically created by using the copy source information and without requiring you to specify monitoring destination information and HUB-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
```

-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

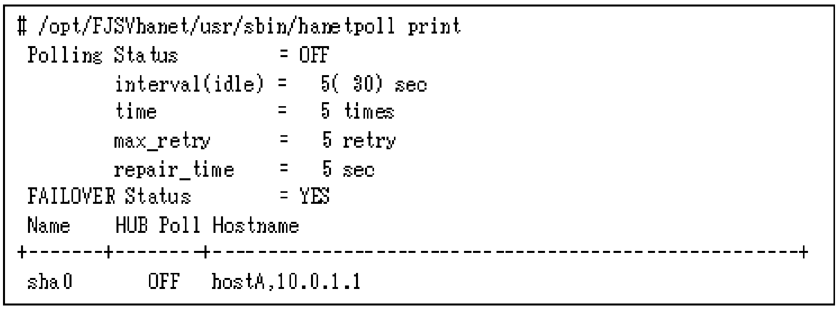
Use the print command to display the current monitoring destination information. Use this command to view the current monitoring destination information. The following is the format of the print command.

```
/opt/FJSVhanet/usr/sbin/hanetpoll print [-n devicename1,devicename2...]
```

devicename1,devicename2...:

Specify the names of virtual interfaces whose monitoring destination information should be displayed. If this option is not specified, the print command displays all the monitoring destination information currently specified.

The following shows an example of displaying information without any option specified.



```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
 Polling Status         = OFF
        interval(idle) =   5( 30) sec
        time           =   5 times
        max_retry      =   5 retry
        repair_time    =   5 sec
 FAILOVER Status        = YES
 Name    HUB Poll Hostname
+-------+-------+---------------------------------------------------+
 sha0       OFF   hostA,10.0.1.1
```

Polling Status : Displays the current status of the monitoring function.

ON : The monitoring function is enabled.
OFF : The monitoring function is disabled.

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 Status : With or without cluster switching when an error occurred in all transfer routes.

YES : Node switching is performed when the virtual interface is registered in the cluster resource.

NO : No node switching is performed.

Name : Displays the name of a virtual interface to be monitored.

HUB Poll : Displays the inter-HUB monitoring status.

ON : The monitoring function is enabled.

OFF : The monitoring function is disabled.

--- : The monitoring function is not used.

Hostname : Displays the host name or IP address to be monitored, in the order of the primary and secondary monitoring destinations. In the example, "hostA" is the primary monitoring destination and "10.0.1.1" is the secondary monitoring destination.

(4) modify command

Use the modify command to modify the monitoring destination information.

```
/opt/FJSVhanet/usr/sbin/hanetpoll modify -n devicename {-p
polladdr1[,polladd2]} | {-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 polladdr1[,polladdr2]:

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.

(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:

```
/opt/FJSVhanet/usr/sbin/hanetpoll on [-s sec] [-c time] [-r retry] [-b sec]
[-f yes | no] [-p sec]
```

-s sec:

Specify the monitoring time in seconds. A value from 1 to 300 can be specified (note that the product of sec and time must be 300 or less). If this option is not specified, the previous setting is enabled. Initially, 5 (seconds) is specified.

-c time:

Specify the monitoring count. A value from 1 to 300 can be specified (note that the product of sec and time must be 300 or less). If this option is not specified, the previous setting is enabled. Initially, 5 (times) is specified.

-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.

This parameter need not be specified for a virtual interface in NIC switching mode (operation mode "d") because "1" (fixed) is set for it.

-b sec:

When detected an error in HUB-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 NIC switching mode. A value from 1 to 300 can be specified. If this option is not specified, the previous setting is enabled. Initially, 60 (seconds) is specified. If the specified value is less than the monitoring interval multiplied by the monitoring count, the system ignores the specified link-up time and adopts the time obtained by multiplying the monitoring interval by the monitoring count.

(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
```

[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/HUB monitoring function may not operate properly.
- Before monitoring destination information can be specified using this command, configuration information must be set using the hanetconfig command.
- This command can be specified for a virtual interface in 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.)
- After modifying monitoring destination information, disable the router/HUB monitoring function (hanetpoll off) and then enable it again (hanetpoll on). If the router/HUB monitoring function is enabled while it has already been enabled (duplicated activation of hanetpoll on), no monitoring destination information is reflected after modification.
- A virtual interface to be used in the cluster system is monitored only while a service to which the virtual interface belongs is in operation.
- If a virtual interface to be monitored is set to Fast switching mode, an error message is output to indicate this fact and the line is not monitored.
- The monitoring time and count to be specified using the hanetpoll on command must be specified so that their product does not exceed 300.
- The retry count to be specified using the hanetpoll on command can be set to 0 from 99999. Monitoring continues indefinitely if 0 is specified.
- Use the hanetpoll print command to display the latest user-defined information (result of create, delete, modify, on, and off) but not to display the current status of 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, not a create command, for setting the second and after. If used a create command, occasionally the state is not displayed properly by a dsppoll command.
- When specified a host name to where to set a host name or an IP address with this command, not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts file. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control Function to use the corresponding host name and to set the definition again.
- When specified a host name with this command to where a host name or an IP address should be set, it is not possble to change/delete a corresponding host name on the database such as /etc/inet/hosts or /etc/inet/ipnodes files. To change/delete 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 specify a multicast address as a monitor-to address.
- When using more than one IPv6 physical interface on the same system, do not specify an IPv6 link local address as a monitor-to address.

[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 shows an example of copying monitoring destination information on virtual interface sha0 to sha1 in NIC switching mode. In the monitoring destination information, PHUB (Primary HUB) and SHUB (Secondary HUB) are already defined as the primary and secondary monitored HUBs.

```
# /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
```

(7) off command

The following shows an example of stopping the router/HUB monitoring function.

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

7.8 dsppoll Command

[Name]

dsppoll - Displaying the monitoring status

[Synopsis]

/opt/FJSVhanet/usr/sbin/dsppoll [-c]

[Feature description]

The dsppoll command displays the current monitoring status of monitoring information created using the hanetpoll or hanetobserv command.

[Option]

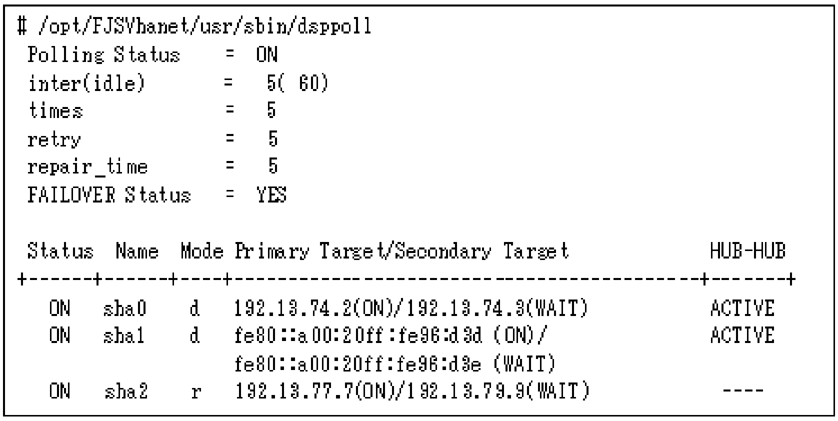
You can specify the following options:

-c

Displays monitoring destination information in GS/SURE linkage mode (operation mode "c") created using the hanetobserv command.

[Display format]

The following shows the display format used when no option is specified.



```
# /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   192.13.74.2(ON)/192.13.74.3(WAIT)          ACTIVE
   ON   sha1    d   fe80::a00:20ff:fe96:d3d (ON)/              ACTIVE
                    fe80::a00:20ff:fe96:d3e (WAIT)
   ON   sha2    r   192.13.77.7(ON)/192.13.79.9(WAIT)           ----
```

Polling Status : Displays the current status of the monitoring function.

- ON : The monitoring function is enabled.
- OFF : The monitoring function is disabled.

interval (idle) :

- 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 : With or without cluster switching when an error occurred in all transfer routes.

- 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.

- ON : Monitoring is in progress.
- OFF : Monitoring is stopped.

Name : Displays the name of a virtual interface to be monitored.

Mode : Displays the operation mode of a virtual interface to be monitored.

- 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/ Secondary Target : Displays monitoring status in Primary/Secondary monitor-to IP address or a host name and parenthesis.

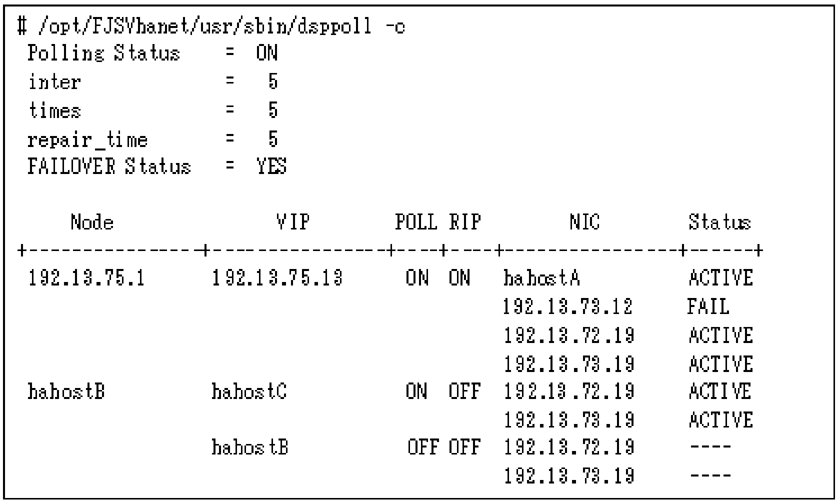
- ON : Monitoring is in progress.
- WAIT : Waiting is in progress.
- FAIL : Monitoring failed (monitoring is stopped).
- CUT : Unused.

HUB-HUB : Displays the status of HUB-HUB communication monitoring.

- ACTIVE : Monitoring is in progress.
- FAIL : Monitoring failed.
- WAIT : Initial status.
- OFF : Monitoring is not yet performed.
- ---- : Monitoring destination not specified.

Hostname : Displays a monitor-to host name or IP address in order of a monitor-to by Primary and that by Secondary. In the case of an example of outputting, "hostA" is a monitor-to by Primary and "10.0.1.1" is that by Secondary.

The following is the display format of monitoring status obtained when the -c option is specified.



```
# /opt/FJSVhanet/usr/sbin/dsppoll -c
 Polling Status    =  ON
 inter             =   5
 times             =   5
 repair_time       =   5
 FAILOVER Status   =  YES

    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     ----
```

Polling Status : Displays the current status of the monitoring function.

ON : The monitoring function is enabled.
OFF : The monitoring function is disabled.

inter : Displays the monitoring interval.

times : Displays the monitoring count.

repair_time : Displays the recovery monitoring interval in seconds.

FAILOVER Status : With or without cluster switching when an error occurred in all transfer routes.

YES : Node switching is performed when the virtual interface is registered in the cluster resource.

NO : No node switching is performed.

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.

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.

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.

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 define d using the hanetpoll command.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
```

(2) The following shows an example of displaying all the monitoring statuses properly define d using the hanetobserv command.

```
# /opt/FJSVhanet/usr/sbin/dsppoll -c
```

7.9 hanetnic Command

[Name]

hanetnic - Dynamic addition/deletion/switching of real interfaces

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetnic command [args]

[Feature description]

The hanetnic command can add, delete, or switch real interfaces to be used dynamically while the relevant virtual interface is active.

Command	Process outline	Authority
add	Adds real interfaces	Super user
delete	Deletes real interfaces	Super user
change	Changes real interface used	Super user

(1) add command

This command adds real interfaces bundled by a virtual interface in Fast switching mode dynamically. (Real interfaces are added while the virtual interface is active.) However, only real 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 interfacename [-f]
```

-n devicename:

Specify a virtual interface name to which the real 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 interfacename:

Specify the real interface name to be added. The interface name specified here must have been set in configuration information for the relevant virtual interface.

-f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic addition.)

(2) delete command

This command deletes real interfaces bundled by a virtual interface in Fast switching mode dynamically (Real interfaces are deleted while the virtual interface is active). However, only real 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 interfacename [-f]
```

-n devicename:

Specify a virtual interface name to which the real 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 interfacename:

Specify the real interface name to be deleted. The interface name specified here must have been set in the configuration information for the relevant virtual interface.

-f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic deletion.)

(3) change command

This command changes real 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 real 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 real 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 real 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 real 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 and converting the environment definition files

[Synopsis]

/opt/FJSVhanet/usr/sbin/hanetrestore -f backupfilename [-v version]

[Feature description]

The hanetrestore command restores the environment definition files used by Redundant Line Control Function. This command also converts the file format of the definition files so they can be used in this version.

[Option]

You can specify the following options:

-f backupfilename

Specify a file created using the backup command.

-v version

Specify the version of Redundant Line Control Function that has executed the backup command.

If this option is omitted, package version 2.3 (product version 4.0) is assumed.

[Related commands]

hanetbackup

[Notes]

- To restore a definition file saved using version 2.3 and later, specify in the "-v" option of the hanetrestore command the version of Redundant Line Control Function used to save the definition file.
- After executing this command, be sure to reboot the system.
- If a file saved using the backup command is restored, the file format is converted at the same time so the file can be used in this version.
- 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.

[Examples]

The following shows an example of restoring a file (/tmp/hanet20020830.bk) created using the backup command on Redundant Line Control Function (FJSVhanet) 2.4 to Redundant Line Control Function (FJSVhanet) 2.4.

```
# /opt/FJSVhanet/usr/sbin/hanetrestore -f /tmp/hanet20020830.bk [-v 2.4]
```

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.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename [-i takeover-ip]
```

-n devicename:

Specifies a name of a virtual interface in Fast switching mode or NIC switching mode created by hanetconfig command. In Fast switching mode, it is possible to set more than one takeover IP to a name of one virtual interface.

-i takeover-ip:

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.

(2) delete command

Deletes the information of a virtual interface from the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n devicename
```

-n devicename:

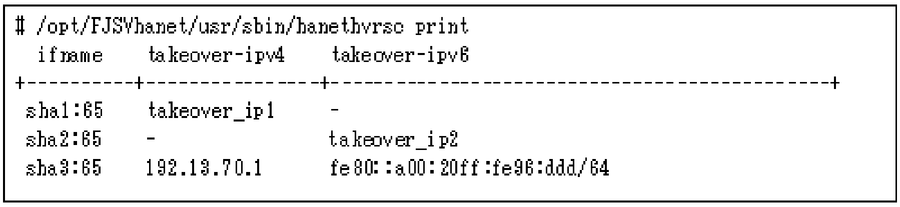
Specifies a name of a logical virtual interface created by create command (shaXX:YY). However, not possible to delete while RMS is working.

(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
```

An example of a display is as follows:



```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
  ifname    takeover-ipv4    takeover-ipv6
+----------+----------------+--------------------------------------------+
 sha1:65    takeover_ip1     -
 sha2:65    -                takeover_ip2
 sha3:65    192.13.70.1      fe80::a00:20ff:fe96:ddd/64
```

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, not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts file. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control Function to use the corresponding host name and to set the definition again.

[Examples]

(1) create command

An example of using create command when setting Fast switching mode:
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 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
```

(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 initialized the configuration information by this command, it is not possible to return to the status immediately before the initialization. When initializing, temporarily saving the information by hanetbackup command is recommended if necessary.

Appendix A List of Error Messages

Appendix A explains the messages that Redundant Line Control Function provides as output.

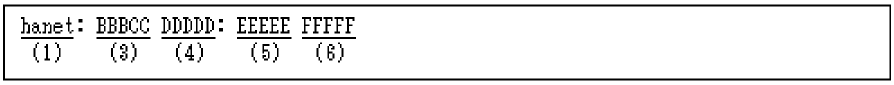
A.1 Messages Displayed by Redundant Line Control Function

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:

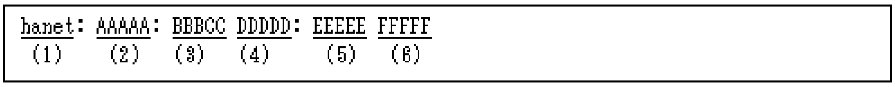
[Output message]

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

Console messages and internal information output messages output this, but not by other messages. The output information (AAAAA) is as follows:

ERROR:

Means that an output message is an error.

WARNING:

Means that an output message is a warning.

INFO:

Means that an output message is the information. This massage is output only when "3.3.8.3 Setting a history of the workings of an interface's up/down" is set.

TRACE:

This indicates internal information output messages.

(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.

(5) Others

The complimentary information (FFFFF) is occasionally output if necessary.

A.1.1 Information message (numbers of 0)

Message number	Message	Meaning	Action
000	normal end.	Execution of the command was successfully completed.	None

A.1.2 Error output message (numbers of 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.	An unauthorized user performed the operation.	Only a user with superuser privilege can perform this operation.
102	this interface is already linked.	The specified virtual device has already been activated.	Execute the dsphanet command to make sure that the virtual interface is in the activated status.
103	resource already exists.	The specified resource has already been registered.	Execute the clgettree command provided by the cluster to confirm the resource ID or resource name you want to specify. Then, specify the correct resource ID or resource name for re-execution.
104	invalid group parent resource id.	Failed to obtain the basic information for the resource.	Execute a clgettree command provided by a cluster, check a resource ID or a resource name to specify, and execute specifying a right resource ID or a resource name again. When this message is output at setting of the resource in NIC switching mode, check that a virtual IP address of an "-i" option is the same in each node that configures a cluster configuration. If not the same, reset to make it the same, and execute again.
105	invalid ip_address.	An invalid IP address is specified.	Specify the correct IP address for re-execution.
106	too many ip_address on device.	Too many takeover resource IDs are registered.	Delete unwanted resources, and execute the command again.
107	invalid resource id.	An invalid resource ID was found.	Execute the clgettree command provided by the cluster to confirm the correct resource ID you want to specify. Then, specify the correct resource ID for re-execution.
108	could not get resource information	Failed to obtain the resource information.	Execute the clgettree command provided by the cluster to confirm the correct resource ID you want to specify. Then, specify the correct resource

	information.		ID for re-execution.
109	specified resource could not operate, because service is not stopped.	Resource operation was rejected because the service is not stopped.	Execute the clgettree command provided by the cluster, or pull up the cluster operation management view and check the operation of the service that has the virtual interface you want to delete.
110	resource has been set to service tree still.	The specified source has been set on the resource service tree.	Delete the service, and execute the command again.
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 deactivated.	Execute the dsphanet command to check the status of the specified virtual interface.
119	interface is active.	The specified virtual interface has been activated.	Execute the dsphanet command to check the status of the specified virtual interface.
120	invalid device name.	An invalid virtual interface name is specified.	Specify the correct virtual interface name, and execute the command again.
121	directory not found.	The specified directory was not found.	Specify a directory name that already exists, and execute the command again.
122	backup file not found.	The specified backup file was not found.	Specify a backup file that already exists, and execute the command again.
123	invalid backup file.	The specified backup file is invalid.	Specify the backup file that was created by the hanetbackup command, and execute the command again.
124	not directory	Directory name was not found where directory was expected.	Specify a directory, and execute the command again.
125	interface is Cluster interface.	The specified interface is available in the cluster operation.	Specify an interface that is not being used in the cluster operation, and execute the command again.
126	shared resource is not found.	An invalid common resource is specified.	Specify a correct common resource name, and execute the command again.
127	invalid key	An invalid resource key is specified.	Specify a correct resource key, and execute the command again.
128	invalid logicalIP.	An invalid logical IP address is specified.	Specify a correct logical IP address, and execute the command again.
129	logicalIP is already defined.	The specified logical IP address has been specified in configuration information.	Specify a different logical IP address, and execute the command again.

130	logicalIP is not specified.	No logical IP address is specified.	Specify a logical IP address, and execute the command again.
131	primaryIF is not specified.	No primary interface is specified.	Specify a primary interface, and execute the command again.
132	invalid primaryIF.	An invalid primary interface is specified.	Specify a correct primary interface, and execute the command again.
133	physicalIP is not specified.	No physical IP address is specified for the interface.	Specify a physical IP address for the interface, and execute the command again.
134	invalid physicalIP.	The physical IP address of the interface is invalid.	Specify a correct physical IP address, and execute the command again.
135	primary polling address is not specified.	No monitoring destination IP address is specified for the primary interface.	Specify a monitoring destination IP address for the primary interface, and execute the command again.
136	invalid primary polling address.	The monitoring destination IP address of the primary interface is invalid.	Specify a correct monitoring destination IP address, and execute the command again.
137	secondaryIF is not specified.	No secondary interface is specified.	Specify a secondary interface, and execute the command again.
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-HUB communication monitoring is performed is not specified.	Specify whether to perform the HUB-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-HUB communication monitoring is performed.	Specify ON or OFF of the HUB-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	logocalIP is	The specified processing could	Stop the transmission line monitoring, and

	active.	not be performed because the transmission line monitoring of the specified operation set was operating.	execute the command again.
152	logocalIP 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	logocalIP 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-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 16)	The maximum number of real interfaces that a virtual interface can bundle in GS linkage mode is exceeded (maximum 16).	Reduce the number of bundled real interfaces, and execute the command again.
159	MAC address is already defined.	The specified MAC address has already been specified.	Specify a different MAC address, and execute the command again.
160	specified devicename could not support cluster.	The specified device does not support cluster operation.	Specify an interface name that support cluster operation, and execute the command again.
161	polling function is defined.	The monitoring function is specified.	Delete a monitoring function with the name of the corresponding virtual interface, and execute again.
162	invalid MAC address.	An invalid MAC address is specified.	Specify a correct MAC address, and execute the command again.
163	IP address or Hostname is already defined.	The specified IP address or host name has already been specified.	Specify a different IP address or host name, and execute the command again.
164	interface name is already defined.	The specified interface name has already been specified.	Specify a different interface, and execute the command again.
165	invalid interface name.	An invalid interface name is specified.	Specify a correct interface name, and execute the command again.
166	invalid mode.	An invalid operation mode is specified.	Specify a correct operation mode, and execute the command again.
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.	An invalid host name is specified.	Specify a correct host name, and execute the command again.
169	physical	The specified physical interface	Specify a different physical interface name, and

	interface name is already defined.	name has already been specified.	execute the command again.
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.
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 party 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.	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	The number of the physical interfaces that configures the	Review the number of the physical interfaces that configures a virtual interface, and change a

	interface is already maximum.	specified virtual interface has reached the maximum number possible to bundle. Therefore, not possible to add an actual interface dynamically.	definition using a hanetconfig command if necessary.
189	invalid network address.	The specified network address is invalid.	Check if or not the specified network address matches with that of a virtual interface network using hanetconfig print command. Specify a correct network address again.
190	virtual gateway function is defined.	A virtual gateway function is already set.	Delete a virtual gateway function with the name of the corresponding virtual interface, then execute again.
191	StandbyIP address function is defined.	A function to specify a standby IP address is already set.	Delete a function to specify a standby IP address with the name of the corresponding virtual interface, and execute again.
192	resource monitor process for virtual interface is running.	A resource monitor for the virtual interface is working.	Execute hvshut command provided by a cluster system, halt a resource monitor, and execute again.
193	Specified interface is already linked to IP.	The IP address is already assigned to the specified interface.	Check if or not there is /etc/hostname.interface file. If exists, change a name or delete it. After executed "/usr/sbin/ifconfig interface name unplumb" command, execute the command again.
194	Specified interface is not bundled by a virtual interface.	The specified interface is not defined as the one to configure a virtual interface.	Check the interface that configures a virtual interface using hanetconfig print command. Specify an interface name displayed in the Interface List, and execute the command again.
195	Standby patrol function could not started.	Not possible to execute a standby patrol function.	Check that the system has already recognized all physical interfaces that configure a virtual interface to be monitored by a standby patrol function, and execute again.
196	Standby patrol function is defined.	A standby patrol function is already set.	Delete a standby patrol function of the corresponding virtual interface name, and execute again.
197	specified physical interface is already unlinked.	Activation of the specified physical interface is already deleted.	Using dsphanet command, check that the specified physical interface is not used yet.
198	address family of takeover ip address incompatible.	The specified address form of a takeover IP address (an address family) is not compatible with that of a setting virtual interface.	Make an address form of a takeover IP address compatible with that of a setting virtual interface and execute again.
199	invalid takeover ip address.	The specified takeover IP address is invalid.	Check a value of the specified takeover IP address and execute again.
200	invalid hostname or prefix value.	The specified host name or prefix value is invalid.	Check the specified host name or prefix value and execute again.
201	dual stack interface can not be specified.	Not possible to specify a virtual interface of dual stack configuration.	Delete a difinition 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	interface defined as cluster resource is still	A virtual interface is registered as cluster resources.	Delete the cluster resources and execute again.

	exist.		
204	interface defined as cluster resource is still active.	A virtual interface is active as cluster resources.	Stop RMS and execute again.

[Message number 3xx]

Message number	Message	Meaning	Action
301	could not open configuration file.	Failed to open the configuration information file.	Check whether the creation of configuration information has been completed.
302	invalid interface name.	An invalid virtual interface name was found in configuration information.	Review the configuration information.
303	hostname is not specified.	The host name is not specified in the configuration information.	Review the configuration information.
304	invalid hostname.	An invalid host name is specified in configuration information.	Review the configuration information.
305	trunking interface list is not specified.	The bundled physical interface is not specified in configuration information.	Review the configuration information.
306	invalid interface count(max 8).	The number of physical interfaces to be bundled exceeds the preset value.	Specify 8 or fewer physical interfaces as the number of interfaces to be bundled.
307	interface name is already defined.	The virtual interface name you want to specify has already been defined in the configuration information.	Specify a virtual interface so that it does not conflict with the other interfaces in the configuration information, and execute the command again.
308	physical interface name is already defined.	The physical interface name that you want to bundle in a virtual interface has already defined.	Review the configuration information.
309	interface address is already defined.	The same IP address is specified for more than one virtual interface.	Review the configuration information.
310	invalid physical interface name.	An invalid physical interface name is specified in the configuration information.	Review the configuration information.
311	invalid file format.	An invalid file format was found in configuration information.	Execute the check command for the configuration information, and take the appropriate action according to the output message.
312	parent device name not found.	The configuration information does not contain the virtual interface with the logical virtual interface.	Review the configuration information.
313	invalid mode.	An invalid operation mode is specified in the configuration information.	Review the configuration information.
314	target is not defined.	The destination information for monitoring does not contain the address information of the monitoring destination.	Review the destination information for monitoring.
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	Primary/Secondary interfaces specified the same monitor-to	Review the destination information for monitoring.

	specified.	address.	
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	LogocalIP 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-HUB communication monitoring is performed is not	Review the monitoring destination information and configuration information.

		specified.	
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-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.
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.

[Message number 5xx]

Message number	Message	Meaning	Action
501	socket() fail.	An error was found in the	Check that there is no mistake in the setting of a Redundant Line Control Function and a cluster

		internal system call.	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.
503	could not connect to cluster control facility.	Failed to establish a connection to the control facility of the cluster system.	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.
504	could not release a connection for cluster control facility.	Failed to release a connection to the control facility of the cluster system.	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.
505	could not get resource.	Failed to obtain attribute information for the resource ID.	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.
506	could not get node identifier.	Failed to get a node ID.	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.
507	could not free resource information lists.	Failed to release the resource ID lists.	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.
508	could not free node resource identifier.	Failed to release the node	Check that there is no mistake in the setting of a Redundant Line Control Function and a cluster

		resource information.	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.
509	could not get the address of a symbol in a shared object.	Failed to obtain the address for the common objects.	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	Check that there is no a mistake in the setting of a

		found in the internal system call.	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).
520	could not add resource.	Failed to register the resource.	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.
521	could not get node information.	Failed to get the basic information of a node.	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.
522	could not set resource attribute.	Failed to create the attribute information for the specified resource.	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.
523	LanDev class resource is not found.	LanDev class resources were not found.	Check there is no mistake in the setting of a Redundant Line Control Function and a cluster system. As for the actual interface to use in a Redundant Line Control Function, when the actual interface name (hme0, qfe0, etc.) is not displayed by /etc/opt/FJSVcluster/bin/clgettree command which does not exist in cluster resources, see "D.4.9 Not possible to register cluster resources", and register in cluster resources. 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 a cluster system, tell Fujitsu SE an error message.
524	could not change attribute for LanDev class resource.	Failed to change the attribute for LanDev class resources.	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.

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).
526	could not set resource information.	Failed to create the basic information for the specified resource.	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.
527	could not free resource identifier lists.	Failed to release the resource ID lists.	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.
528	could not get resource id.	Failed to obtain the resource ID lists.	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.
529	could not delete resource.	Failed to delete the resource.	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.
530	could not get shared resource information.	Failed to get the basic information of the shared resource.	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.
531	invalid resource name.	The resource name is invalid.	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.
532	could not get resource attribute	Failed to obtain the resource	Check that there is no mistake in the setting of a Redundant Line Control Function and a cluster

	attribute.	attribute.	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.
533	could not free resource attribute lists.	Failed to release the resource attribute list.	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.
534	resource attribute is not set.	No attribute information exists in the resource.	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.
535	HAnet_Device class resource is not found.	The HAnet_Device class resource was not found.	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.
536	could not get resource status on service tree.	Failed to obtain the specified resource status.	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.
537	could not replace a service parent resource id.	Failed to change the parent resource on the resource service tree.	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.
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 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).
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. 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. 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.	Collect materials for examination of a Redundant Line Control Function, and tell Fujitsu SE an error message.
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.

A.1.3 Console output messages (numbers of 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	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.
	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	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.

	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).
807	callback regist failed.	Failed to register the cluster call back function.	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.
808	resource attribute get failed.	Failed to obtain the cluster resource attribute.	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.
809	resource attribute set failed.	Failed to set the cluster resource attribute.	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.
810	node information get failed.	Failed to obtain the cluster node information.	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.
811	resource id get failed.	Failed to obtain the cluster resource identifier.	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.
812	resource information get failed.	Failed to obtain the cluster resource information.	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.
813	event parse failed.	Failed to analyze 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.
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.

818	ClStartEvent failed.	Failed to start 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.
819	ClGetEsFd failed.	Failed to obtain the cluster communication FD.	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.
820	ClDispatchEvent failed.	Failed to dispatch 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.
821	ClGetStat failed.	Failed to obtain the cluster resource status.	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	The operation mode of the virtual interface for router monitoring is defined

		monitoring is invalid. Thus, the router monitoring function for this virtual interface cannot be enabled.	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 using the check command of hanetpoll. 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 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.
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	Check the line failure. After checking the line recovery, inactivate and activate the

		specified by the retry count consecutively. The router monitoring function is disabled.	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.
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-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-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-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.(ifname)	A message was received from an unregistered remote system. ifname: Interface name	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.
885	standby interface recovered.(sourceip)	The remote system interface recovered. sourceip: Source address	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 interface. This message is output when the monitor-to information to set by a hanetpoll create command is other than HUB.	Not necessary to deal with. When executing prompt failback, use a hanetpoll modify command and change the monitor-to information to a host name or an IP address of HUB.

[Message number 9xx]

Message number	Message	Meaning	Action
990	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	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	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 linkage script error output messages

In a DR linkage 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 linkage script. The messages displayed in a DR linkage 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	A virtual interface XX that	Delete a definition of the cluster

	interface. The DR processing is stopped. Action=ZZ devicename=XX interface=YY	bundles an interface YY is already registered as the cluster resource. Stops a DR process.	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.

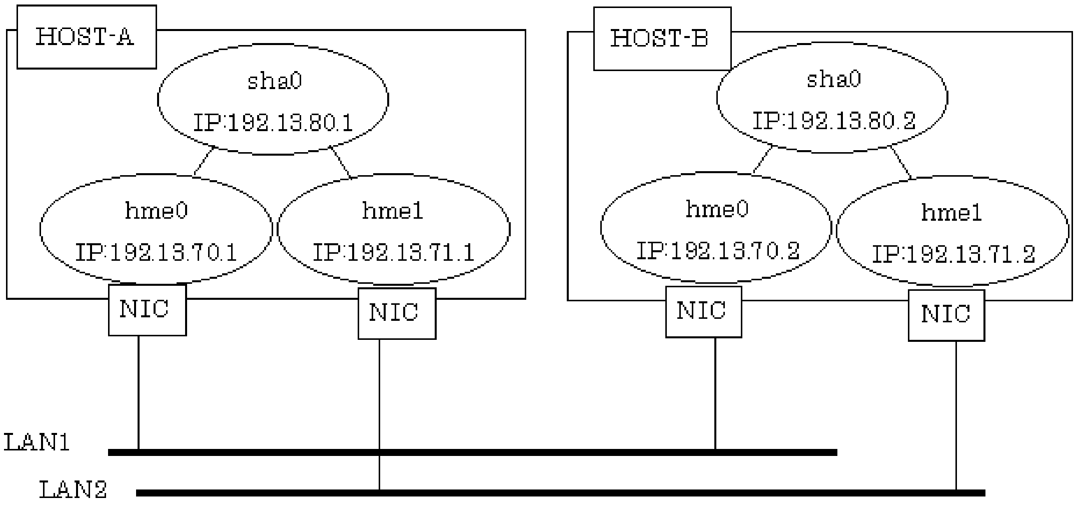
Appendix B Examples of Setting Up

The local IP address is used for the IP address in this definition example.

B.1 Example of Setting up the Redundant Operation by F ast switching mode

B.1.1 Example of the Single system

This section provides an example of setting up in the following network configuration.



[HOST-A]

1) Setting up the Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.1 -t hme0,hme1

2) Separately activating the Virtual interfaces

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

[HOST-B]

1) Setting up the Virtual interface

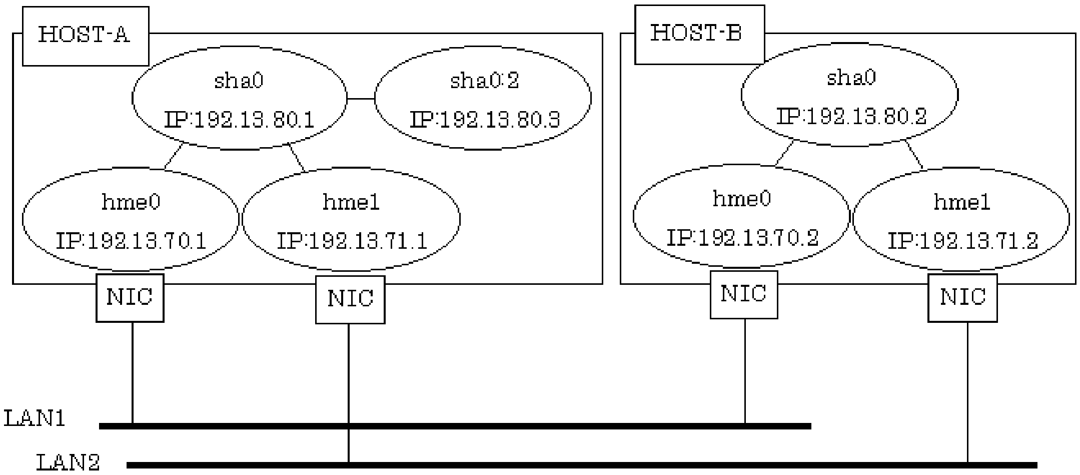
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.2 -t hme0,hme1

2) Separately activating the Virtual interfaces

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

B.1.2 Example of the Single system in Logical Virtual interface

This section provides an example of setting up in the following network configuration.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.1 -t hme0,hme1
```

2) Setting up the Logical Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.13.80.3
```

[HOST-B]

1) Setting up the Virtual interface

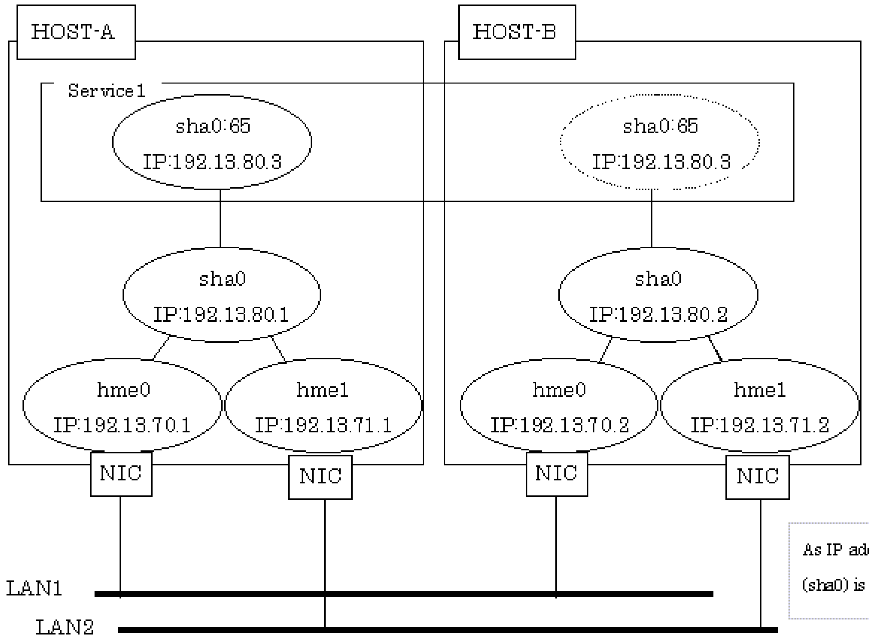
```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.2 -t hme0,hme1
```

2) Separately activating the Virtual interfaces

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

B.1.3 Example of the Cluster system (Standby mode)

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.



As IP address of a virtual interface (sha0) is not taken over.

[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.1 -t hme0,hme1
```

2) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.3
```

3) Setting up the Wizard

To execute after completed "2) Setting up the Cluster configuration" in HOST-B.

4) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.2 -t hme0,hme1
```

2) Setting up the Cluster configuration

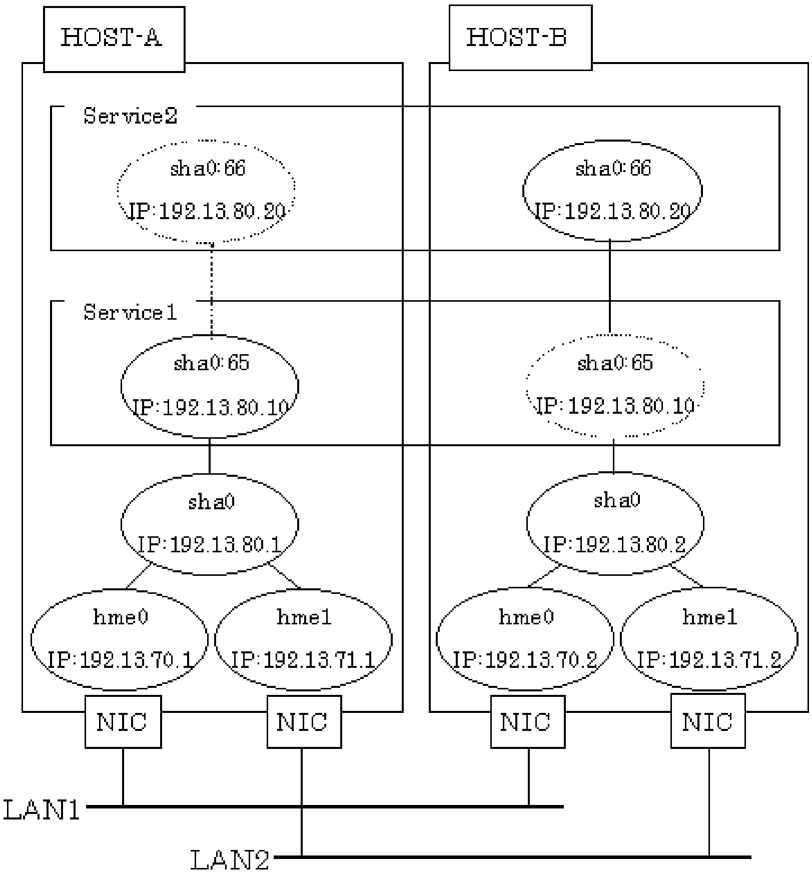
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.3
```

3) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.1.4 Example of the Cluster system (Mutual standby mode)

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.



As IP address of a virtual interface (sha0) is not taken over.

[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.1 -t hme0,hme1
```

2) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.10
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.20
```

3) Setting up the Wizard

To execute after completed "2) Setting up the Cluster configuration" in HOST-B.

4) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.2 -t hme0,hme1
```

2) Setting up the Cluster configuration

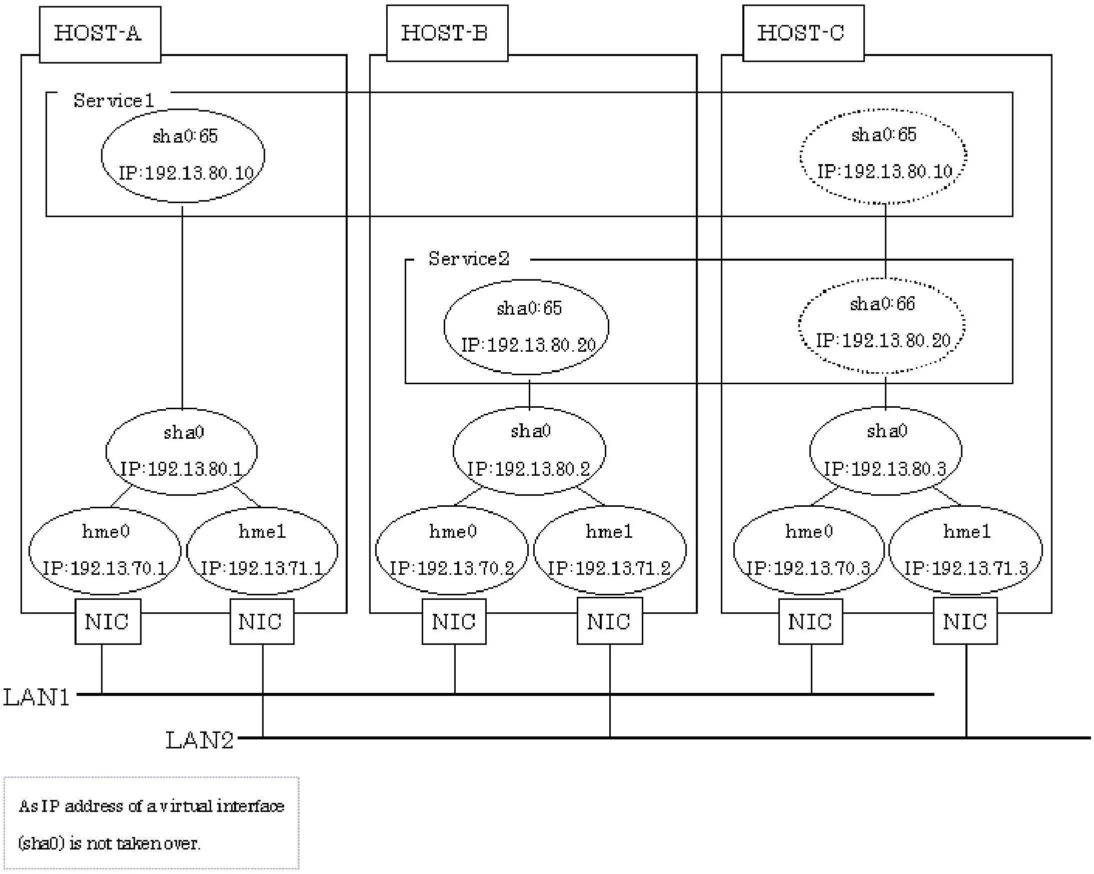
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.10
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.20
```

3) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.1.5 Example of the Cluster system (2:1 standby mode)

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.



[HOST-A]

1) Setting up the Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.1 -t hme0,hme1

2) Setting up the Cluster configuration

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.10

3) Setting up the Wizard

To execute after completed "2) Setting up the Cluster configuration" in HOST-B and HOST-C.

Notes:
When setting up the Wizard at HOST-A, takeover IP address "192.13.80.20" doesn't appear at the menu of Wizard. Please choice "FREECHOICE" and input takeover IP address directly.
Set HOST-B and HOST-C for a host name of the Active node (Machines[0]) and the Standby node (Machines[1]) respectively.

4) Rebooting

When setting up of the HOST-A, HOST-B and HOST-C is complete, reboot all nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.2 -t hme0,hme1
```

2) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.20
```

3) Rebooting

When setting up of the HOST-A, HOST-B and HOST-C is complete, reboot all nodes simultaneously.

[HOST-C]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.3 -t hme0,hme1
```

2) Setting up the Cluster configuration

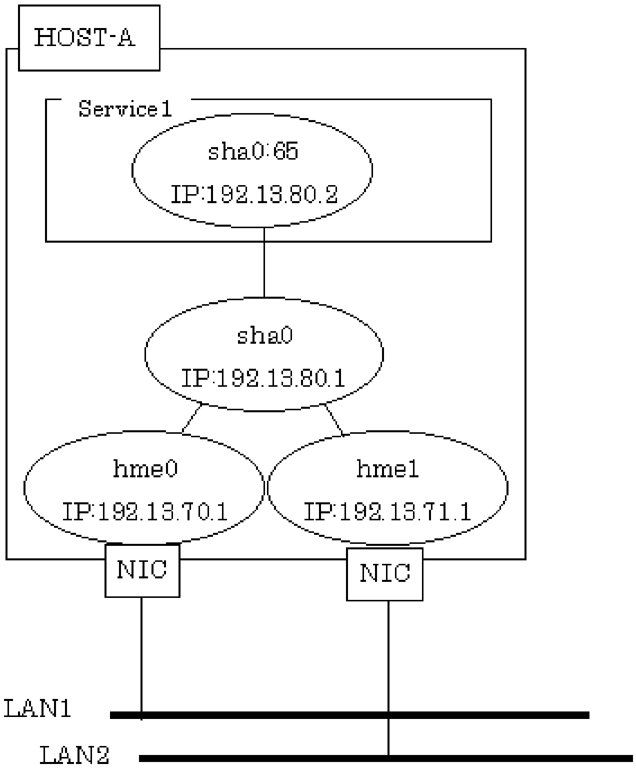
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.10
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.20
```

3) Rebooting

When setting up of the HOST-A, HOST-B and HOST-C is complete, reboot all nodes simultaneously.

B.1.6 Example of the Cluster system (1 node cluster)

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.13.80.1 -t hme0,hme1
```

2) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.13.80.2
```

3) Setting up the Wizard

Set a wizard after completed to set cluster environment. It is not necessary to add a standby node (Machines[1]).

[Notes]
When setting a wizard from a node other than HOST-A in cluster environment configured by more than one node, set a HOST-A host name to an operation node (Machines[0]).

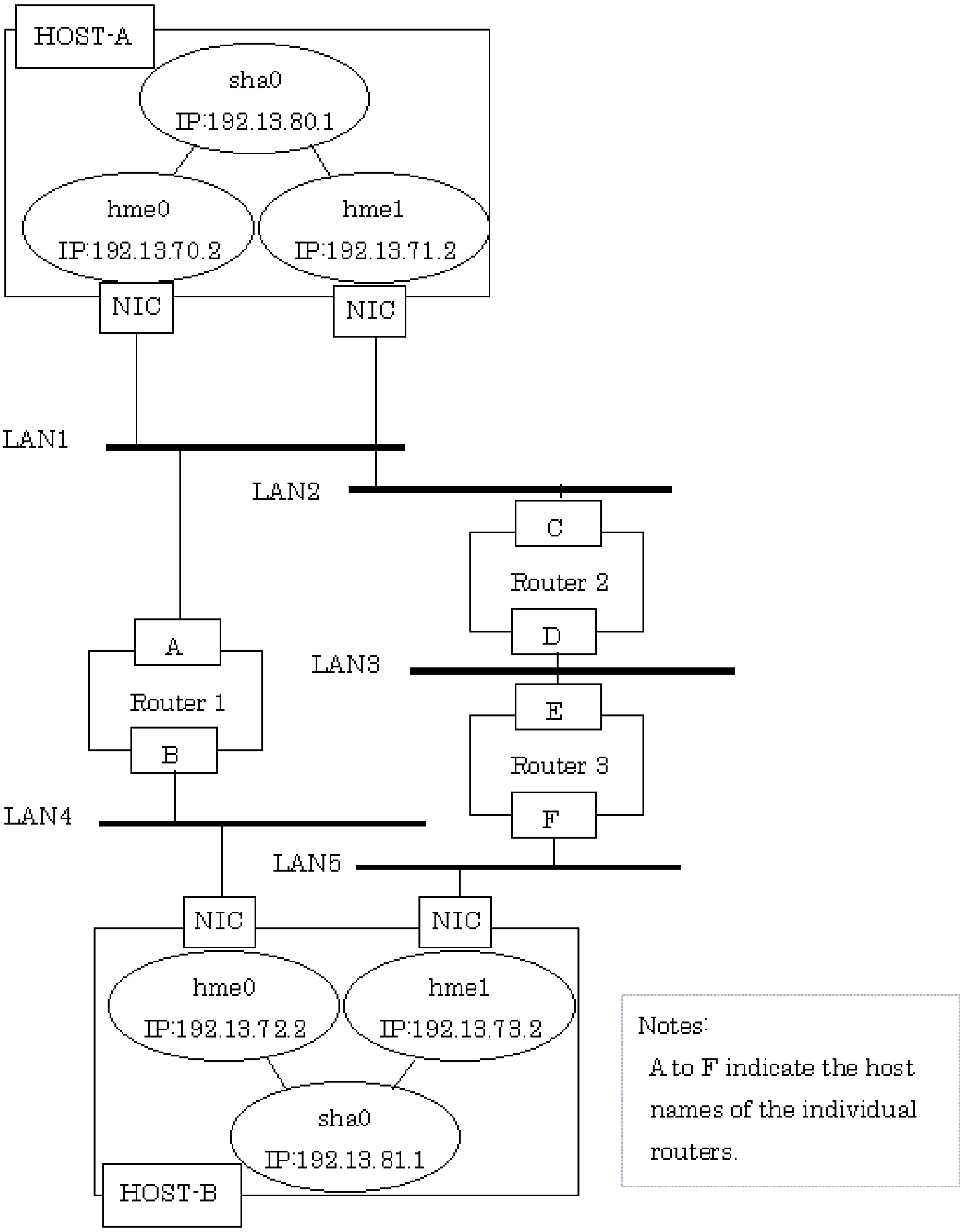
4) Rebooting

Reboot when completed all the environment setting.

B.2 Example of Setting up the Redundant Operation by RI P mode

B.2.1 Example of the Single system

This section provides an example of setting up in the following network configuration.
If the router monitoring function is not used, omit 2) and 4) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i 192.13.80.1 -t hme0,hme1
```

2) Setting up the Router monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p A,C
```

3) Separately activating the Virtual interfaces

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

4) Specifying the start of 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 Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i 192.13.81.1 -t hme0,hme1
```

2) Setting up the Router monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p B,F
```

3) Separately activating the Virtual interfaces

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

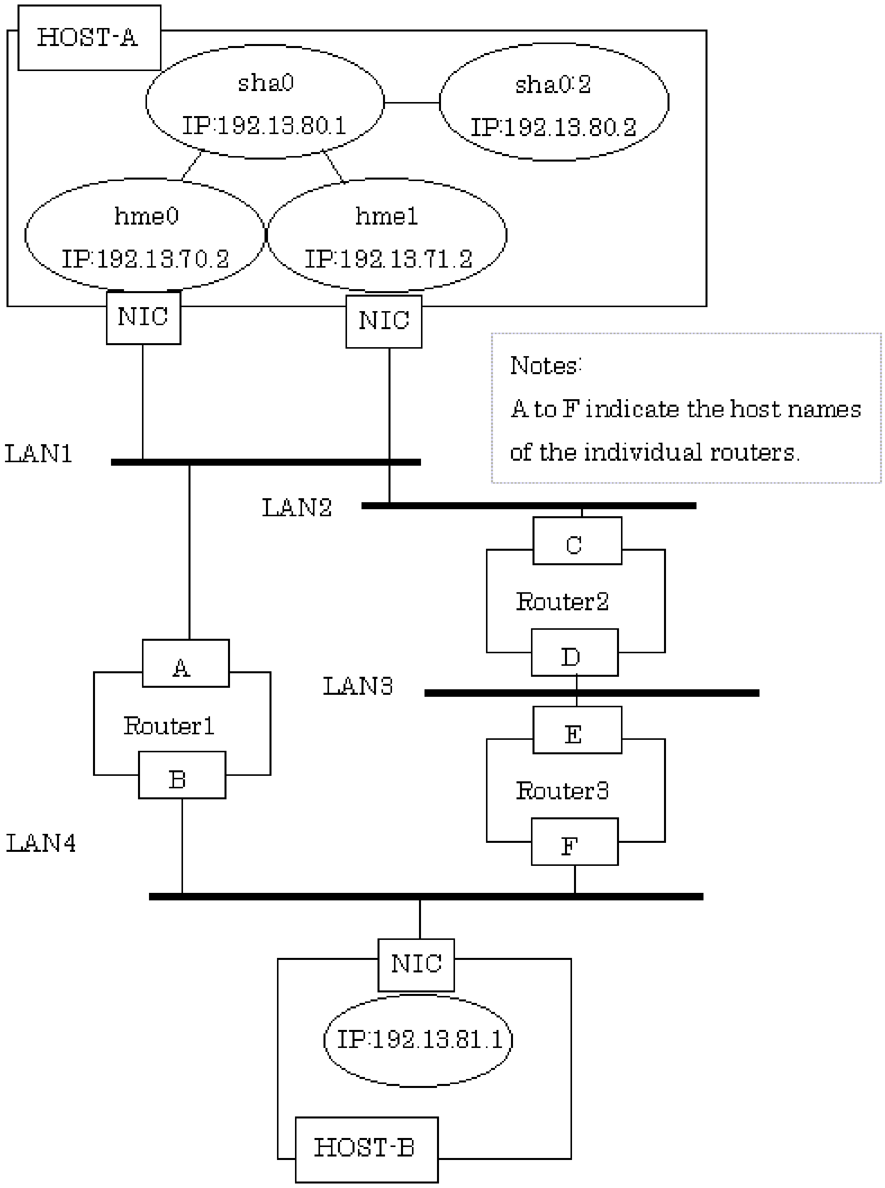
4) Specifying the start of the Router monitoring function

(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.2.2 Example of the Single system in Logical Virtual interface

This section provides an example of setting up in the following network configuration.
If the Router monitoring function is not used, omit 3) and 5) in the procedure for setting up on each host.



Notes:
A to F indicate the host names of the individual routers.

[HOST-A]

1) Setting up the Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m r -i 192.13.80.1 -t hme0,hme1

2) Setting up the Logical Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.13.80.3

3) Setting up the Router monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p A,C

4) Separately activating the Virtual interfaces

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

5) Specifying the start of the Router monitoring function

(To monitor every four seconds. To stop a router monitoring function if failed six times in succession. The example is shown below.)
/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.3 Example of Setting up the Fast switching/RIP mode

B.3.1 Example of the Single system

See the appendix B.1.1 and appendix B.2.1.

B.3.2 Example of the Single system in Logical Virtual interface

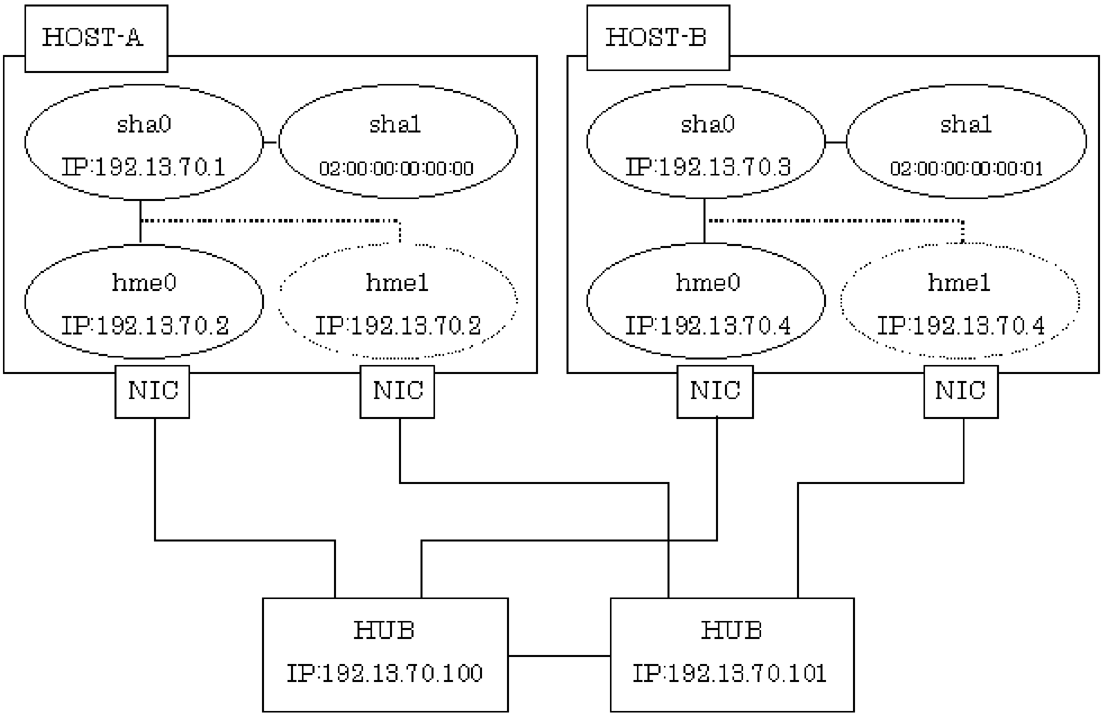
See the appendix B.1.2 and appendix B.2.2.

B.4 Example of Setting up the NIC switching mode (IPv4)

B.4.1 Example of the Single system without NIC sharing

This section provides an example of setting up in the following network configuration.

If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
```

3) 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
```

4) Separately activating the Virtual interfaces

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

5) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.3 -e 192.13.70.4 -t hme0,hme1
```

2) Setting up the HUB-HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
```

3) 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
```

4) Separately activating the Virtual interfaces

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

5) Specifying the start of the HUB monitoring function

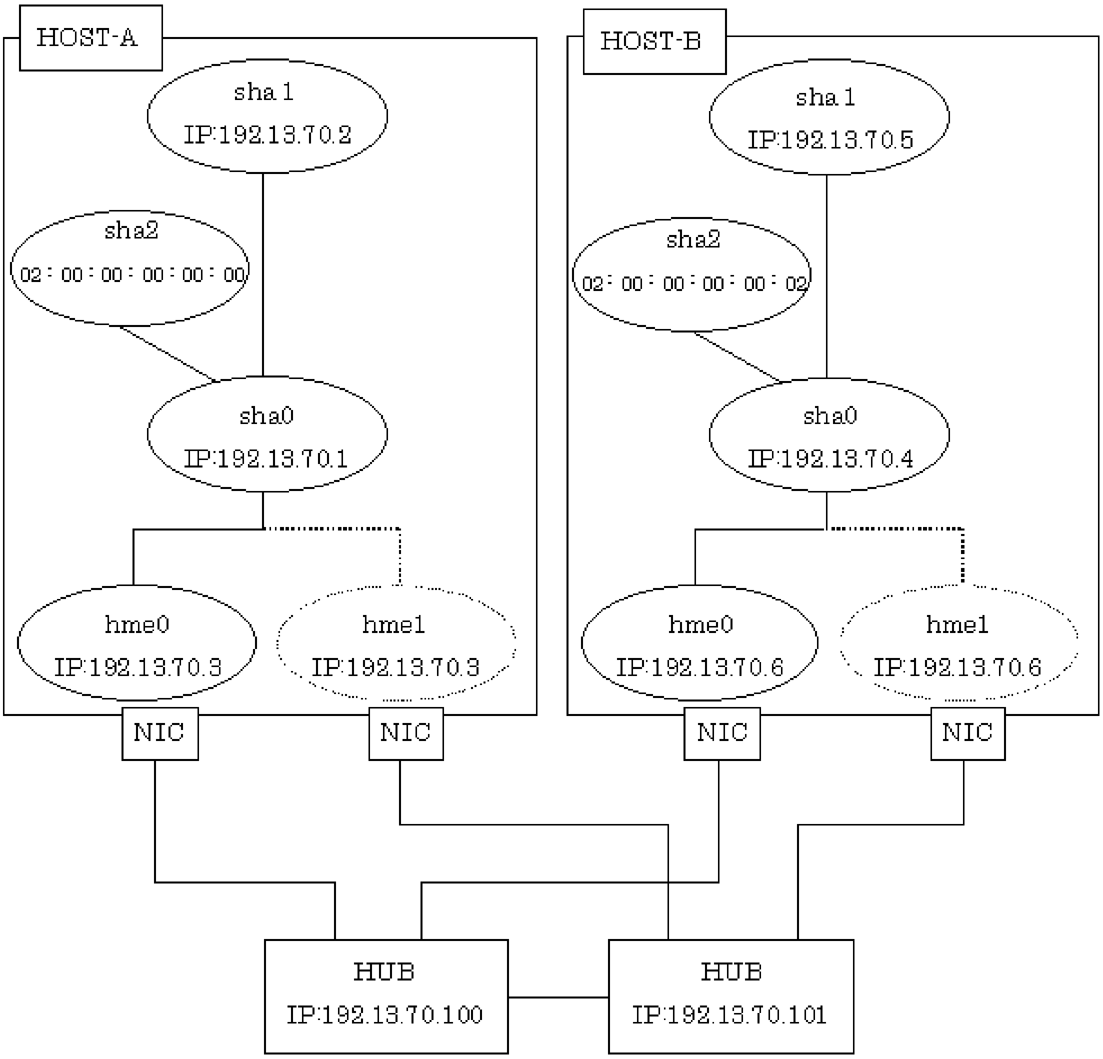
(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

B.4.2 Example of the Single system with NIC sharing

This section provides an example of setting up in the following network configuration.

If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.2
```

2) Setting up the HUB-HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

3) 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
```

4) Separately activating the Virtual interfaces

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

5) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.4 -e 192.13.70.6 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.5
```

2) Setting up the HUB-HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

3) 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
```

4) Separately activating the Virtual interfaces

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

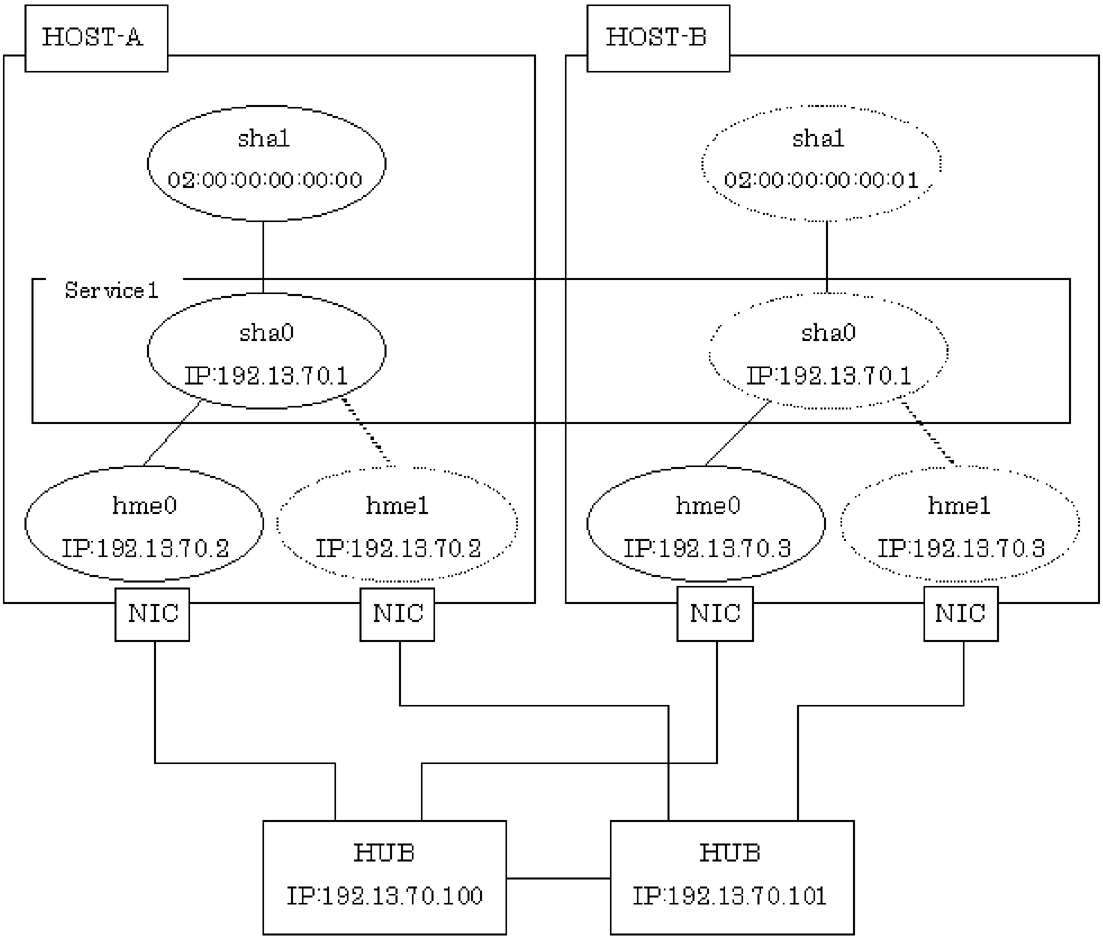
5) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

B.4.3 Example of the Cluster system (Standby mode)

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b off
```

3) 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
```

4) Setting up the Cluster configuration

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

5) Setting up the Wizard

To execute after completed "4) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b off
```

3) 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
```

4) Setting up the Cluster configuration

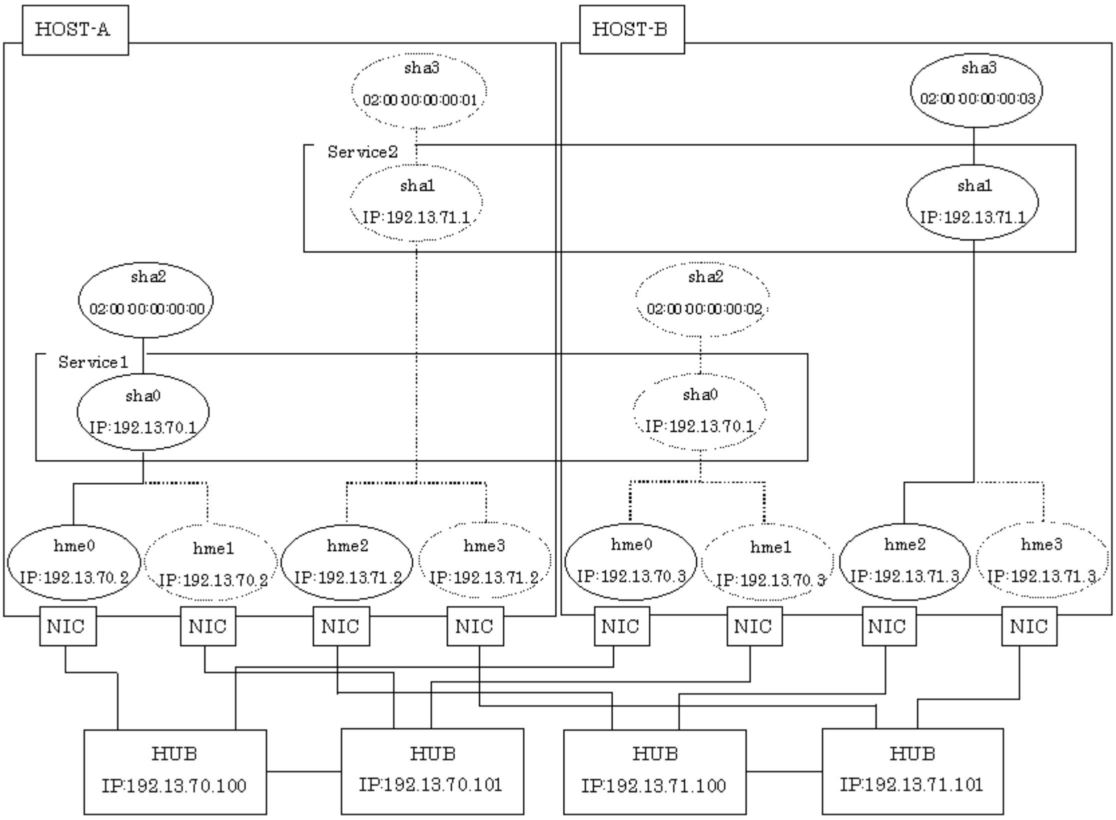
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

5) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.4.4 Example of the Cluster system (Mutual standby mode) without NIC sharing

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.13.71.1 -e 192.13.71.2 -t hme2,hme3
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.13.71.100,192.13.71.101 -b off
```

3) 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
```

4) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

5) Setting up the Wizard

To execute after completed "4) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.13.71.1 -e 192.13.71.3 -t hme2,hme3
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.13.71.100,192.13.71.101 -b off
```

3) 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
```

4) Setting up the Cluster configuration

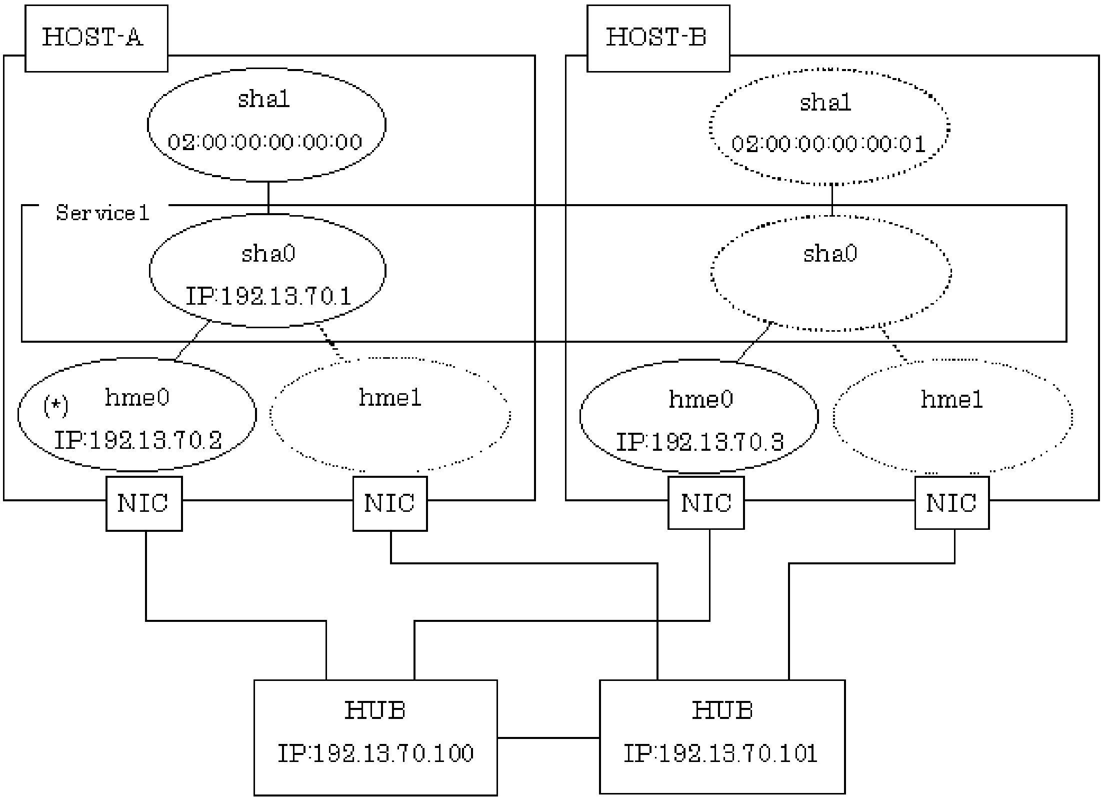
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

5) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.4.5 Example of the Cluster system in takeover physical IP address (pattern I)

This section provides an example of setting up in the following network configuration (Activation physical interface on the Standby node).
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) If a takeover IP:192.13.70.1 activated, a physical IP:192.13.70.2 is not activated.

[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
```

3) 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
```

4) Setting up the Cluster configuration

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

5) Setting up the Wizard

To execute after completed "4) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
```

3) 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
```

4) Setting up the Cluster configuration

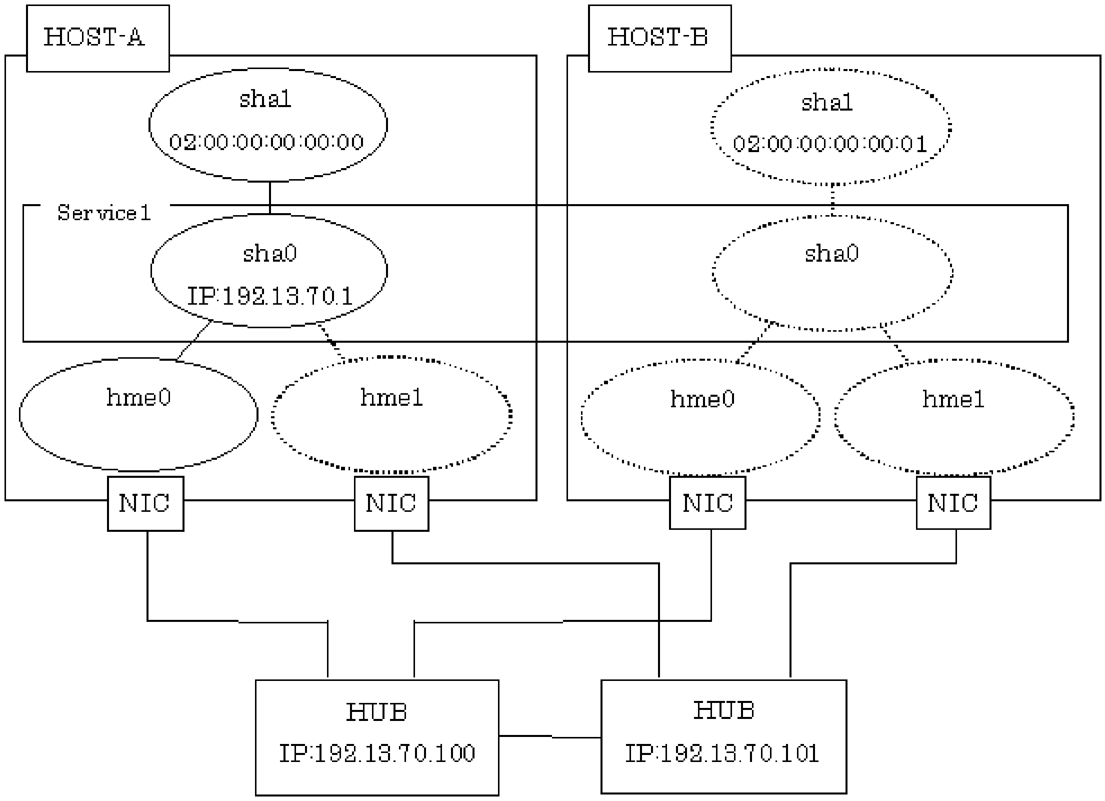
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

5) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.4.6 Example of the Cluster system in takeover physical IP address (pattern II)

This section provides an example of setting up in the following network configuration (Not activation physical interface on the Standby node).
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.13.70.1 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
```

3) 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
```

4) Setting up the Cluster configuration

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

5) Setting up the Wizard

To execute after completed "4) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.13.70.1 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
```

3) 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
```

4) Setting up the Cluster configuration

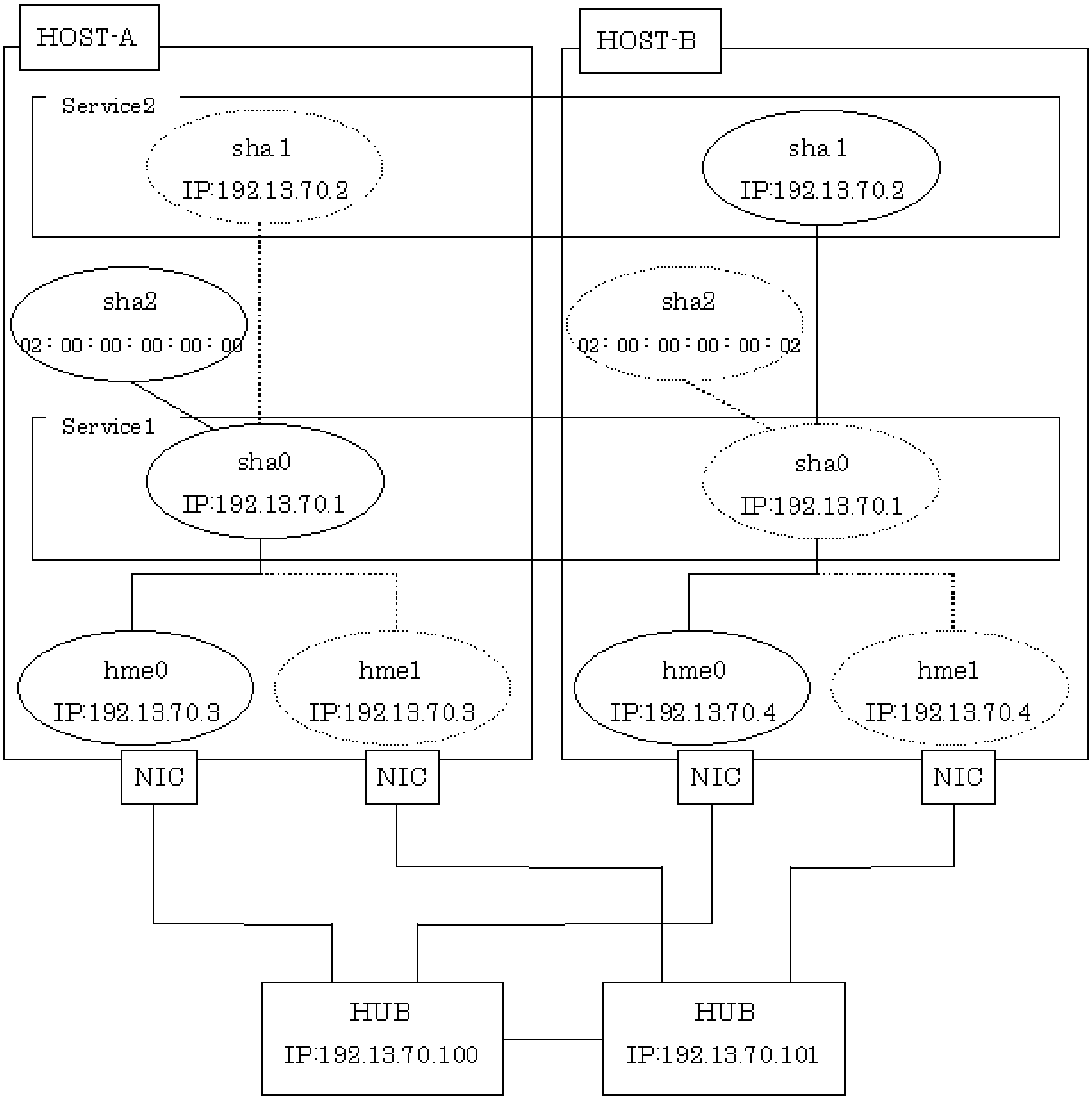
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

5) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.4.7 Example of the Cluster system (Mutual standby mode) with NIC sharing

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.2
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

3) 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
```

4) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

5) Setting up the Wizard

To execute after completed "4) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.4 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.2
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

3) 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
```

4) Setting up the Cluster configuration

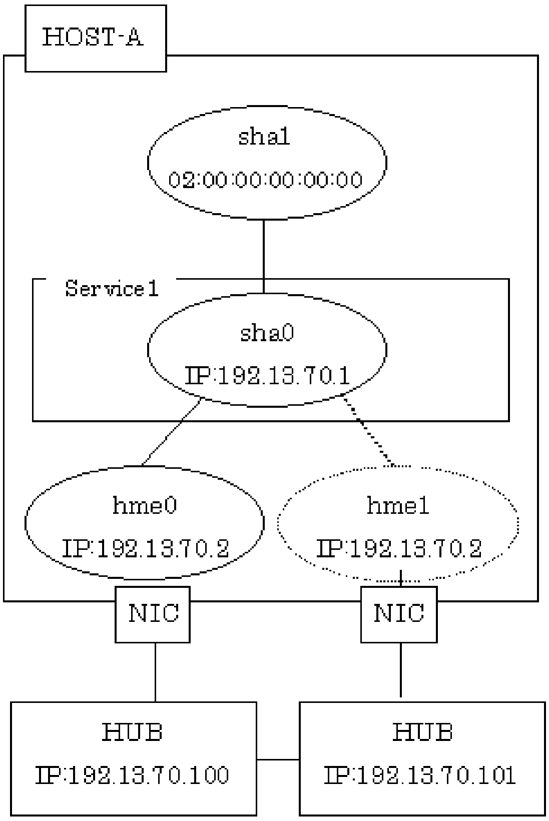
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

5) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.4.8 Example of the Cluster system (1 node cluster)

This section provides an example of setting up in the following network configuration.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b off
```

3) 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
```

4) Setting up the Cluster configuration

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

5) Setting up the Wizard

Set a wizard after completed to set cluster environment. It is not necessary to add a standby node (Machines[1]).

[Notes]
When setting a wizard from a node other than HOST-A in cluster environment configured by more than one node, set a HOST-A host name to an operation node (Machines[0]).

6) Rebooting

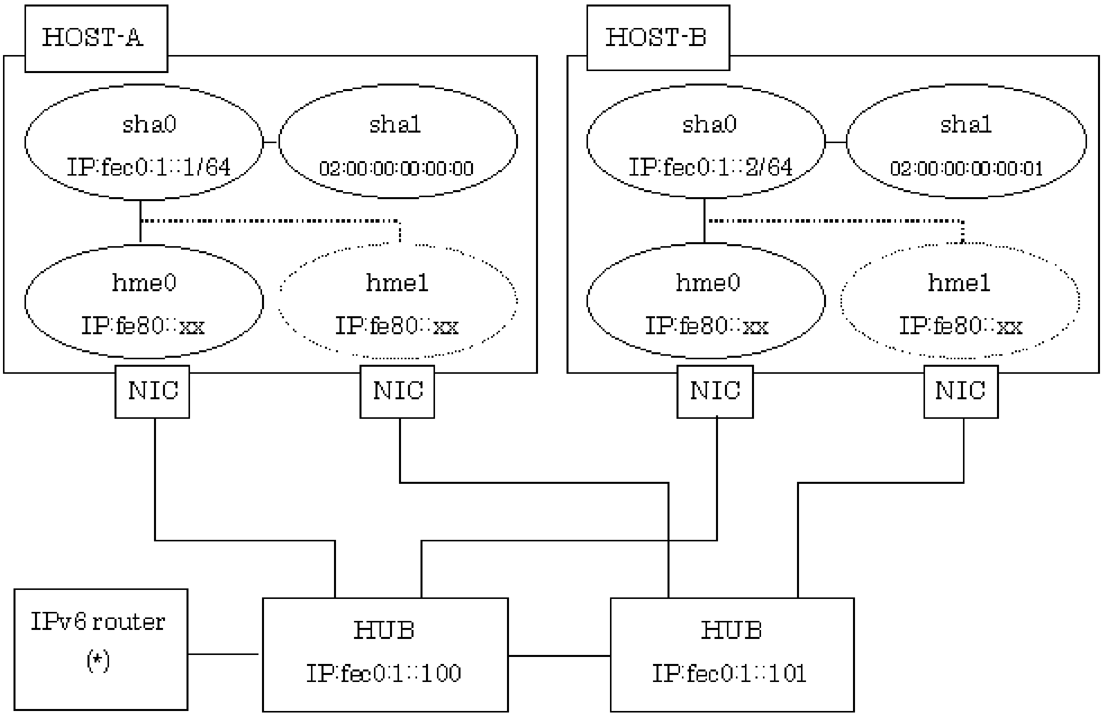
Reboot when completed all the environment setting.

B.5 Example of Setting up the NIC switching mode (IPv6)

B.5.1 Example of the Single system without NIC sharing

This section provides an example of setting up in the following network configuration.

If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

2) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100, fec0:1::101 -b on

3) 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

4) Separately activating the Virtual interfaces

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

5) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5

[HOST-B]

1) Setting up the Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t hme0,hme1

2) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100, fec0:1::101 -b on

3) 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

4) Separately activating the Virtual interfaces

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

5) Specifying the start of the HUB monitoring function

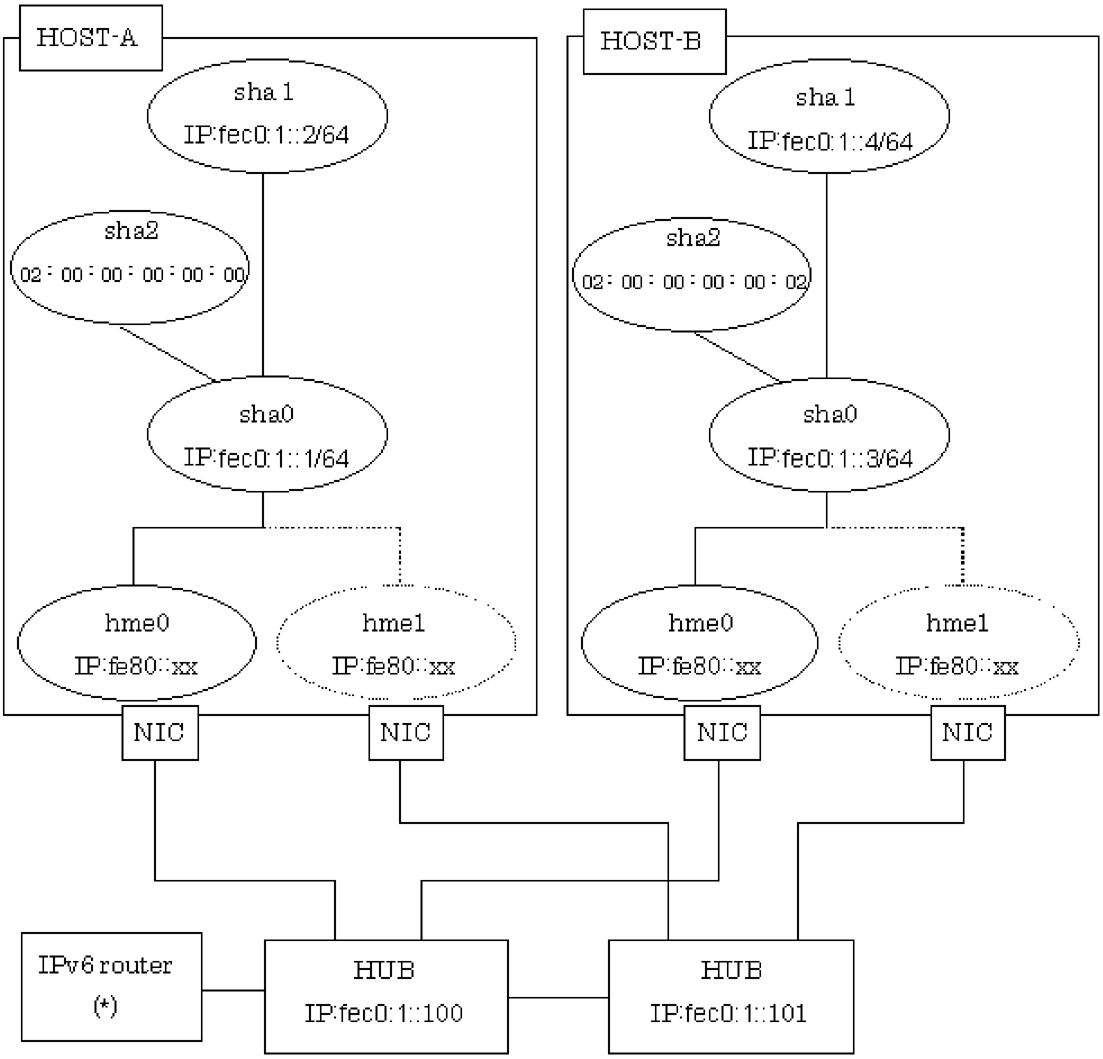
(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5

B.5.2 Example of the Single system with NIC sharing

This section provides an example of setting up in the following network configuration.

If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 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
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100, fec0:1::101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

3) 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
```

4) Separately activating the Virtual interfaces

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

5) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

[HOST-B]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64
```

2) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100, fec0:1::101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

3) 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
```

4) Separately activating the Virtual interfaces

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

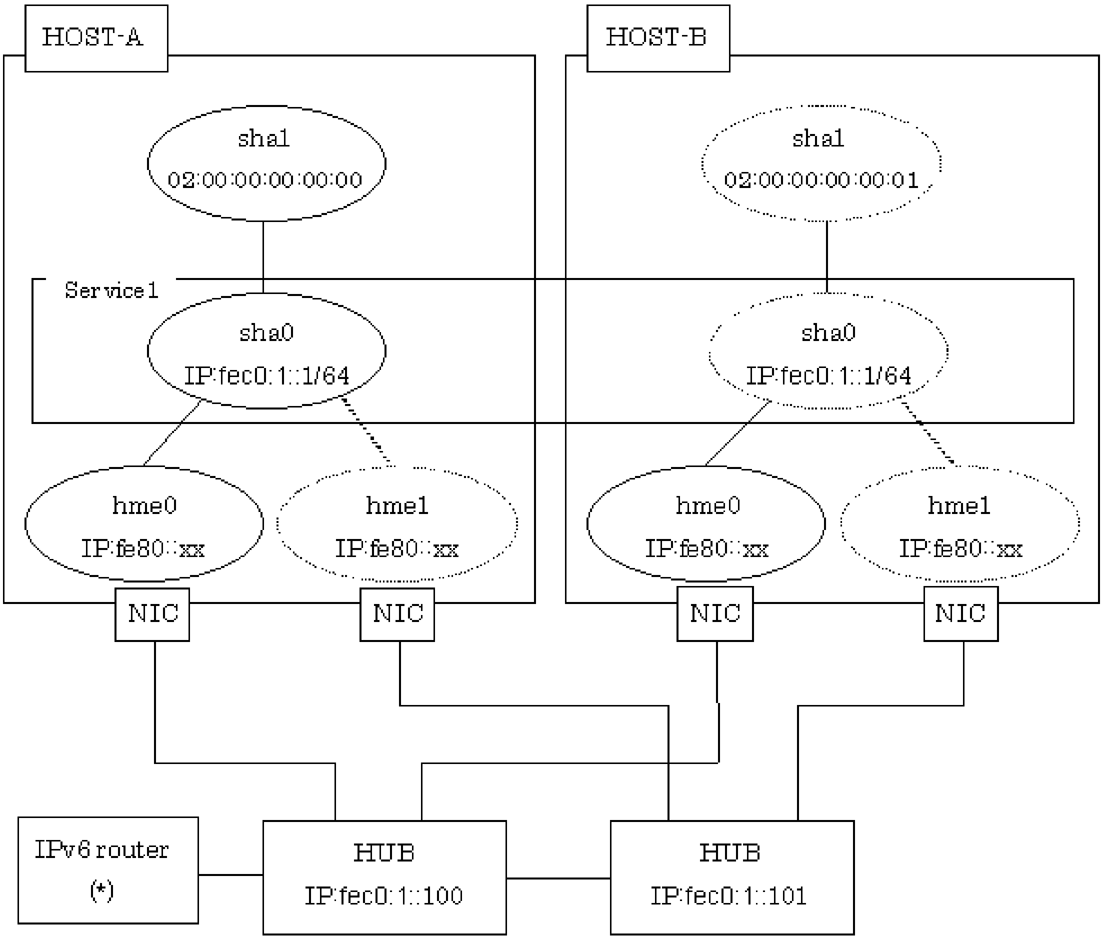
5) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

B.5.3 Example of the Cluster system (Standby mode)

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

2) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100, fec0:1::101 -b off

3) 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

4) Setting up the Cluster configuration

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

5) Setting up the Wizard

To execute after completed "4) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

2) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100, fec0:1::101 -b off

3) 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

4) Setting up the Cluster configuration

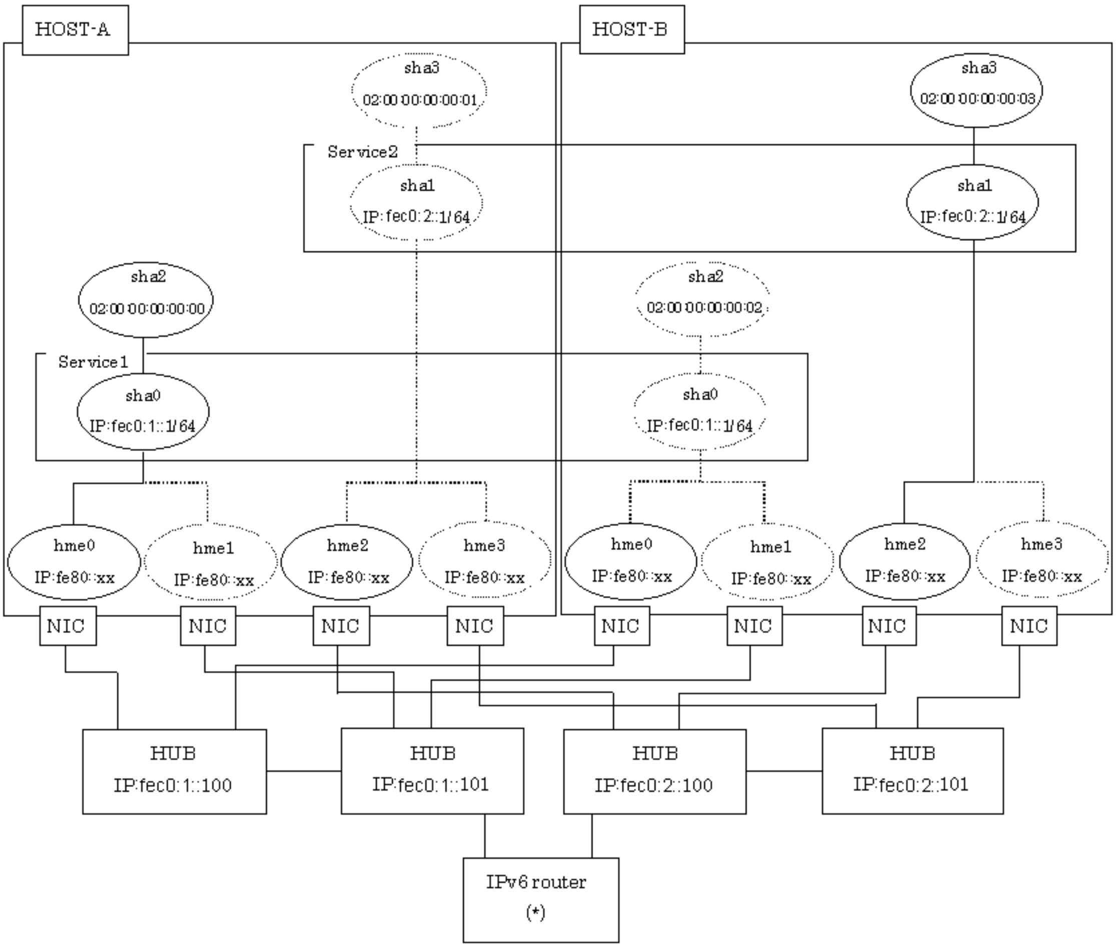
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0

5) Rebooting

```
When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.
```

B.5.4 Example of the Cluster system (Mutual standby mode) without NIC sharing

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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".
```

[HOST-A]

1) Setting up the 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

2) 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 fec0:1::100, fec0:1::101 -b off

3) 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

4) Setting up the Cluster configuration

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

5) Setting up the Wizard

To execute after completed "4) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the 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

2) 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 fec0:1::100, fec0:1::101 -b off

3) 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

4) Setting up the Cluster configuration

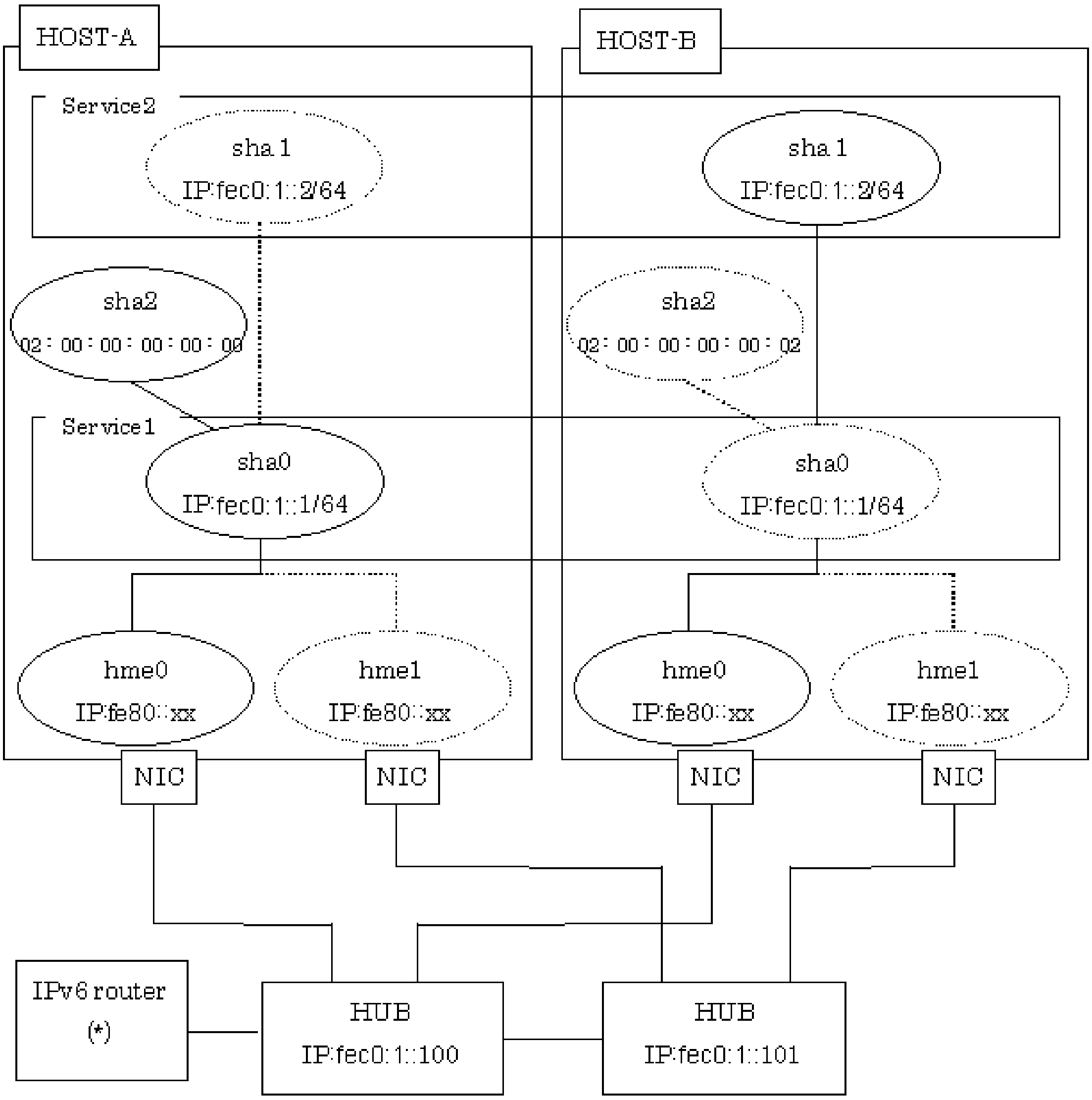
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

5) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.5.5 Example of the Cluster system (Mutual standby mode) with NIC sharing

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 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

2) 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

3) 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

4) Setting up the Cluster configuration

/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1

5) Setting up the Wizard

```
To execute after completed "4) Setting up the Cluster configuration" in HOST-B.
```

6) Rebooting

```
When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.
```

[HOST-B]

1) Setting up the 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
```

2) 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
```

3) 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
```

4) Setting up the Cluster configuration

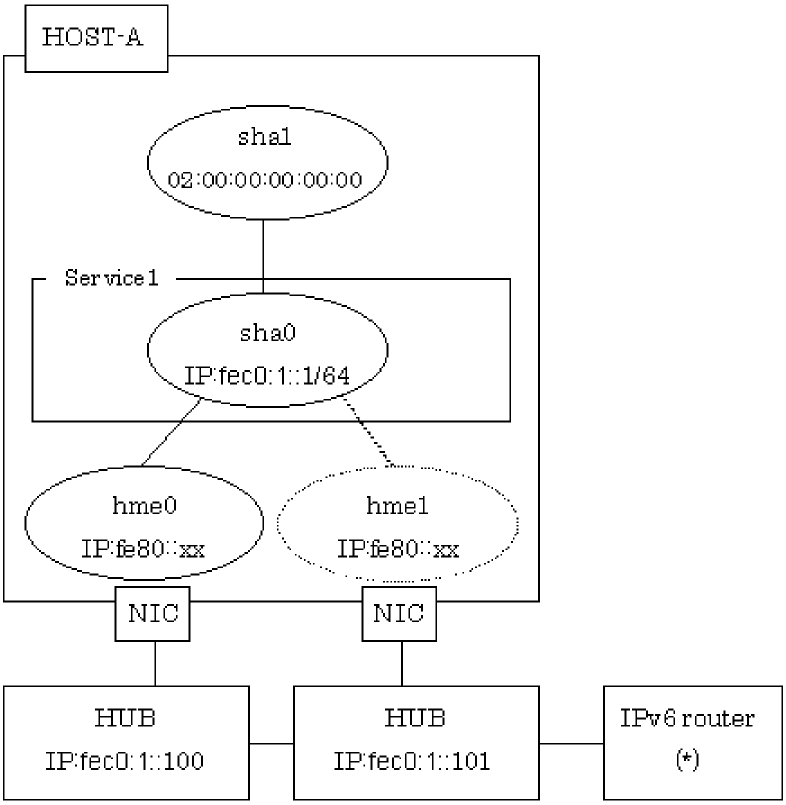
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

5) Rebooting

```
When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.
```

B.5.6 Example of the Cluster system (1 node cluster)

This section provides an example of setting up in the following network configuration.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

2) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100, fec0:1::101 -b off

3) 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

4) Setting up the Cluster configuration

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

5) Setting up the Wizard

Set a wizard after completed to set cluster environment. It is not necessary to add a standby node (Machines[1]).

[Notes]
When setting a wizard from a node other than HOST-A in cluster environment configured by more than one node, set a HOST-A host name to an operation node (Machines[0]).

6) Rebooting

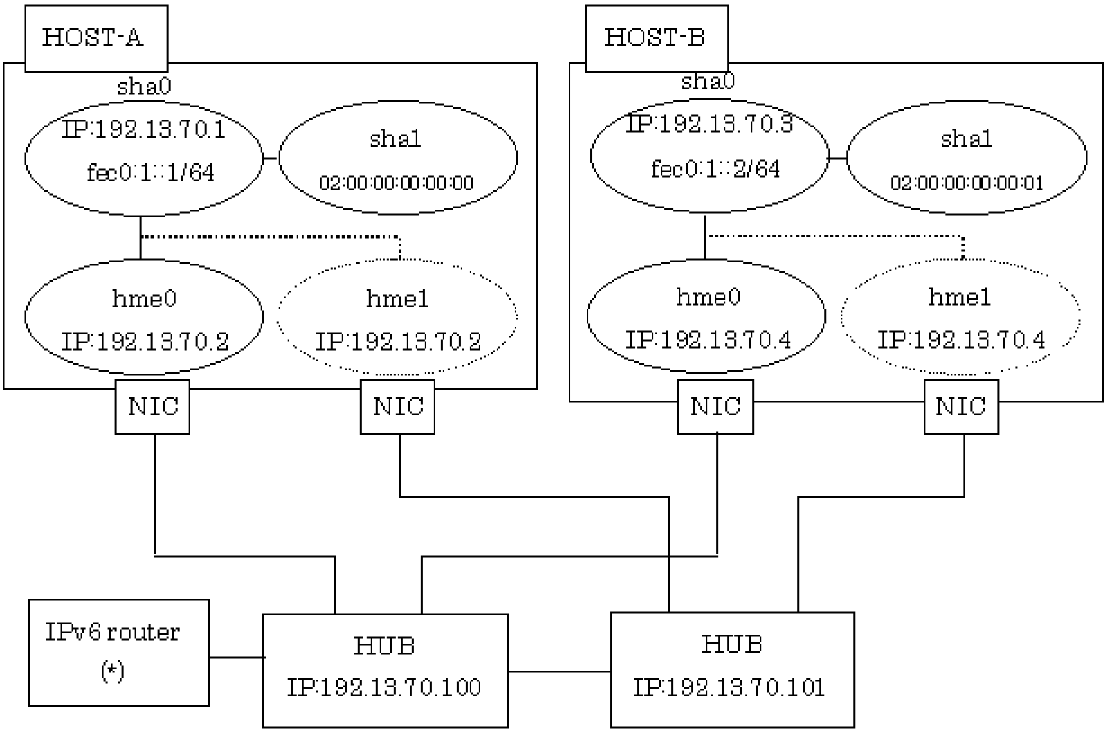
Reboot when completed all the environment setting.

B.6 Example of Setting up the NIC switching mode (IPv4/IPv6 dual stack)

B.6.1 Example of the Single system without NIC sharing

This section provides an example of setting up in the following network configuration.

If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface of IPv4

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1

2) Setting up the Virtual interface of IPv6

/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on

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

[HOST-B]

1) Setting up the Virtual interface of IPv4

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.3 -e 192.13.70.4 -t hme0,hme1

2) Setting up the Virtual interface of IPv6

/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on

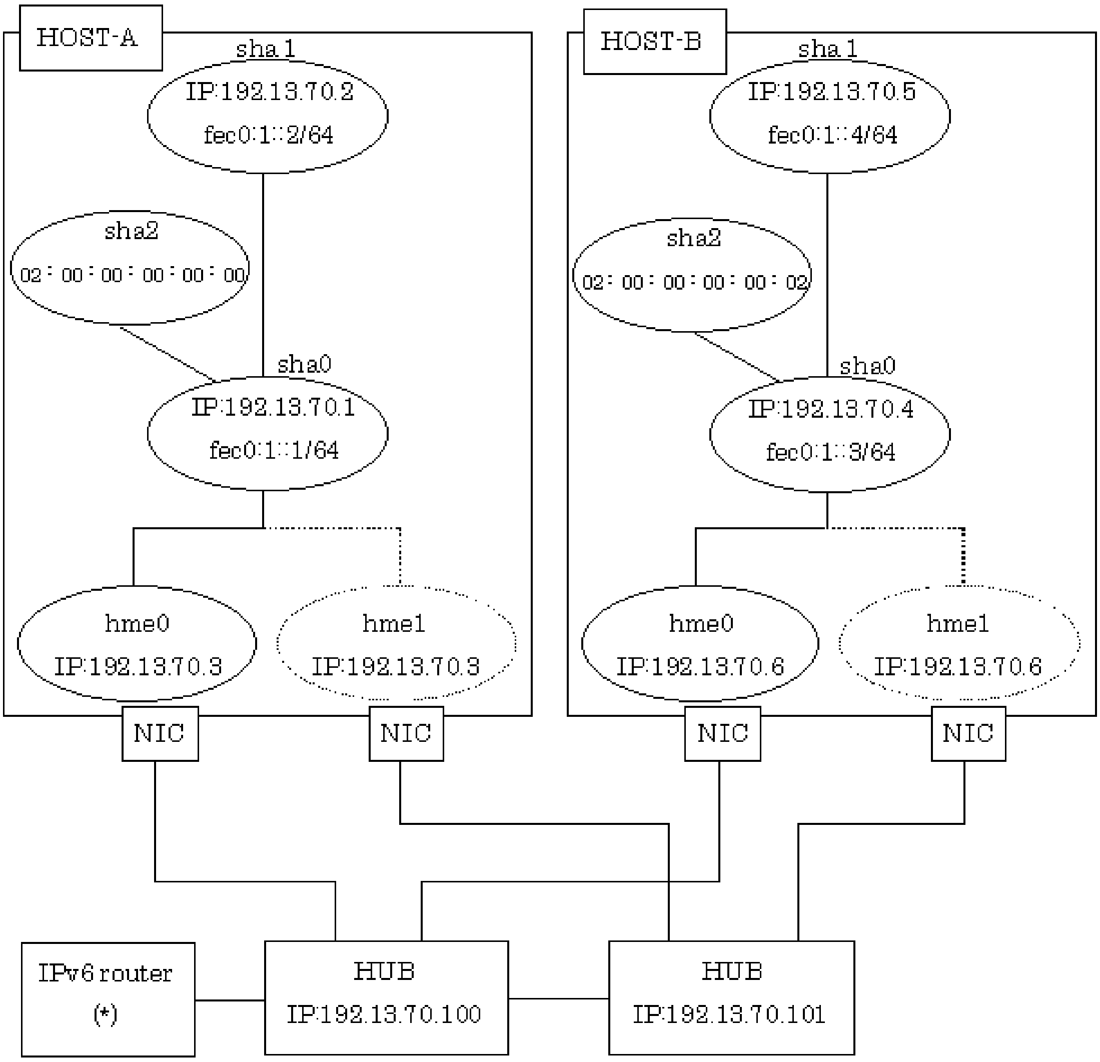
4) Setting up the Standby patrol monitoring function

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -t sha0

B.6.2 Example of the Single system with NIC sharing

This section provides an example of setting up in the following network configuration.

If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.2
```

2) Setting up the Virtual interface of IPv6

```
/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
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

4) 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
```

5) Separately activating the Virtual interfaces

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

6) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

[HOST-B]

1) Setting up the Virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.4 -e 192.13.70.6 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.5
```

2) Setting up the Virtual interface of IPv6

```
/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
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

4) 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
```

5) Separately activating the Virtual interfaces

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

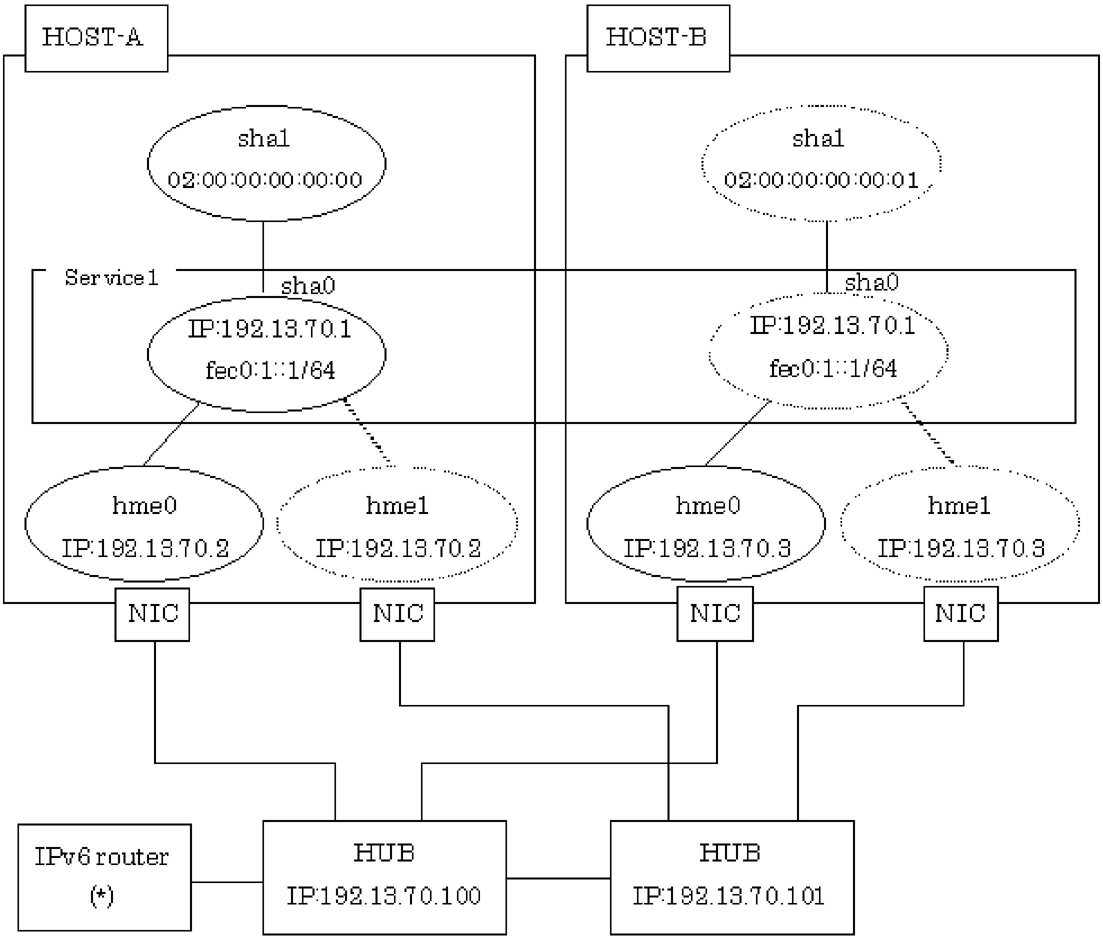
6) Specifying the start of the HUB monitoring function

(The following is an example where monitoring is performed 5 times at the interval of 4 seconds.)

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -s 4 -c 5
```

B.6.3 Example of the Cluster system (Standby mode)

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface of IPv4

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1

2) Setting up the Virtual interface of IPv6

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on

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) Setting up the Cluster configuration

/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha0

6) Setting up the Wizard

To execute after completed "5) Setting up the Cluster configuration" in HOST-B.

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
```

2) Setting up the Virtual interface of IPv6

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
```

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) Setting up the Cluster configuration

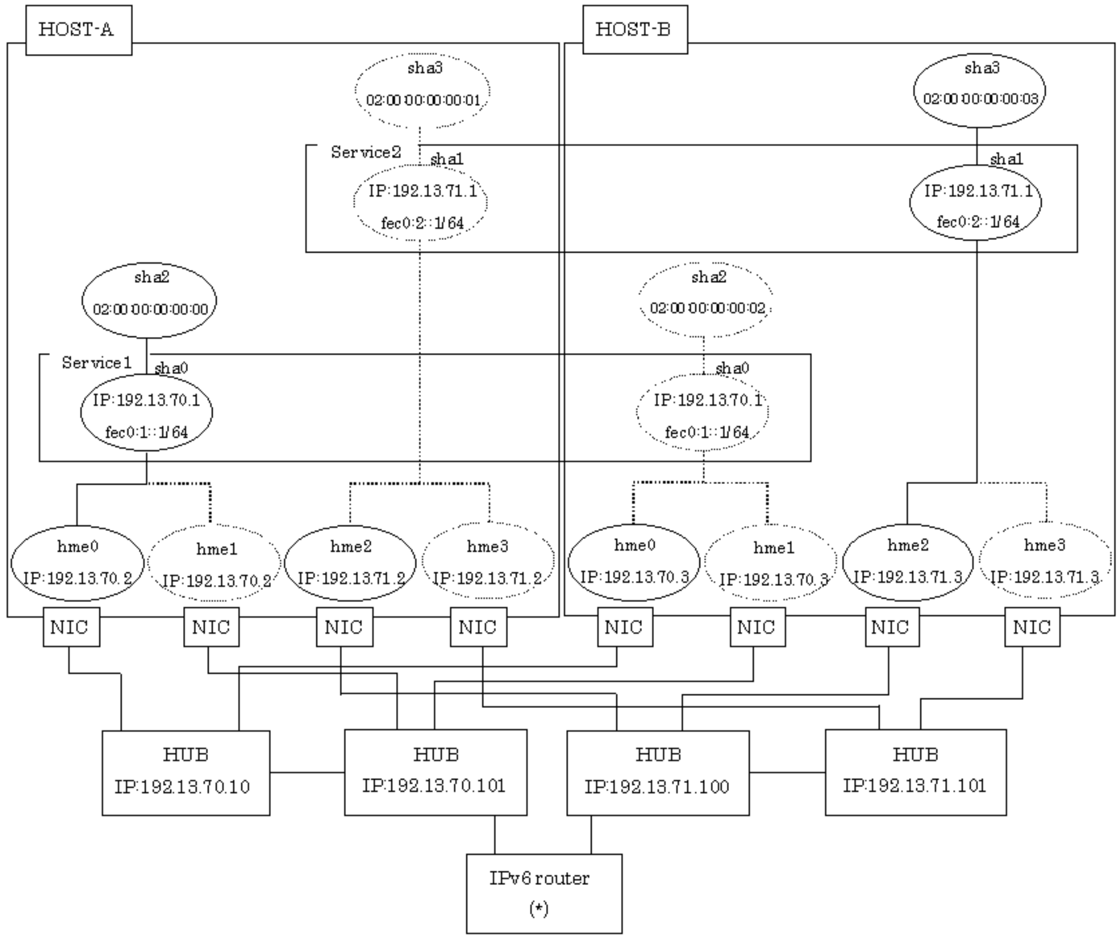
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha0
```

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.6.4 Example of the Cluster system (Mutual standby mode) without NIC shar ing

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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".
```

[HOST-A]

1) Setting up the Virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.13.71.1 -e 192.13.71.2 -t hme2,hme3
```

2) Setting up the Virtual interface of IPv6

```
/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
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.13.71.100,192.13.71.101 -b on
```

4) 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
```

5) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha1
```

6) Setting up the Wizard

To execute after completed "5) Setting up the Cluster configuration" in HOST-B.

7) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.13.71.1 -e 192.13.71.3 -t hme2,hme3
```

2) Setting up the Virtual interface of IPv6

```
/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
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.13.71.100,192.13.71.101 -b on
```

4) 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
```

5) Setting up the Cluster configuration

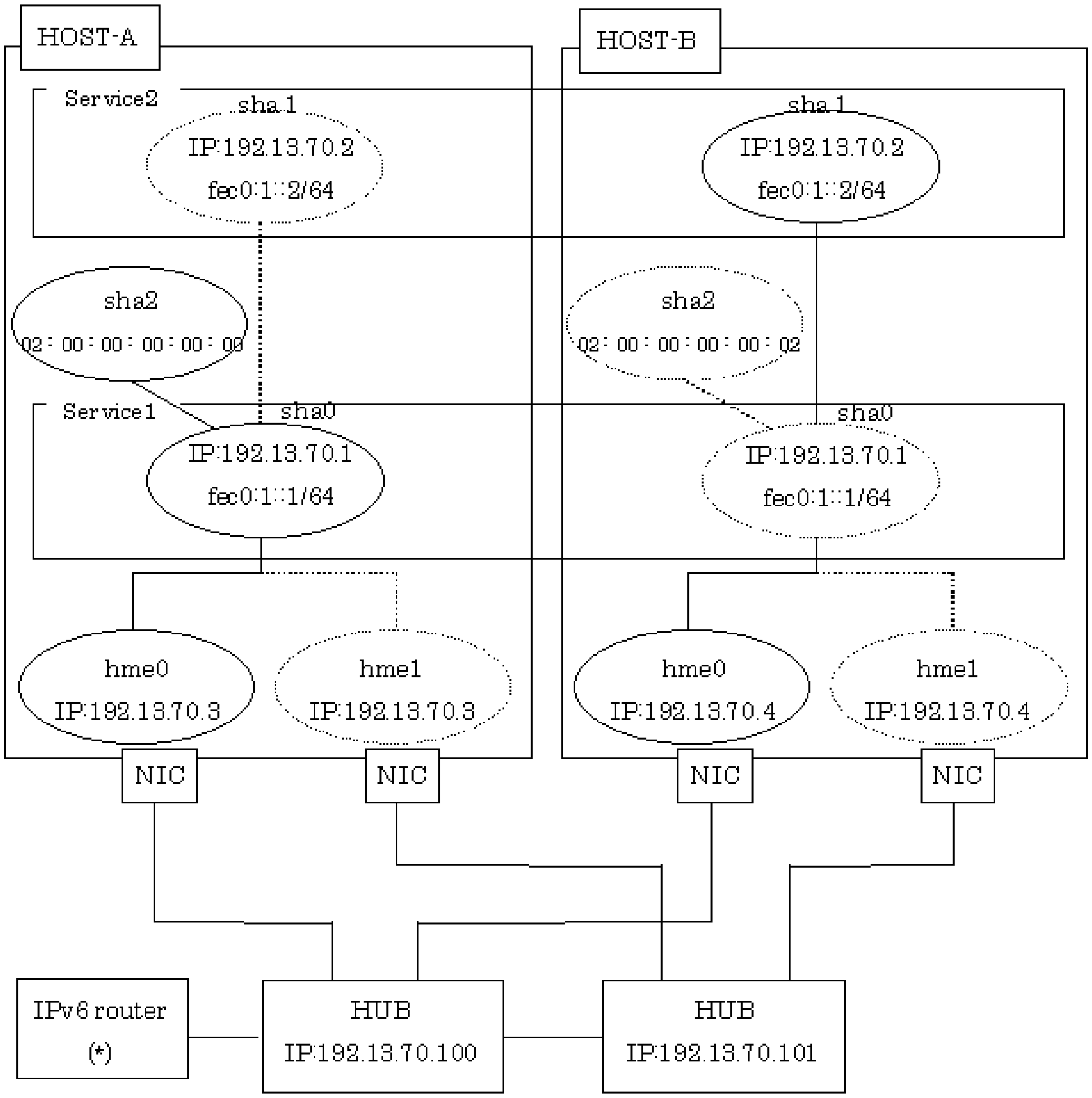
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha1
```

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.6.5 Example of the Cluster system (Mutual standby mode) with NIC sharing

This section provides an example of setting up in the following network configuration.
See such as a Cluster system manual as to the initial setting of a Cluster system and configure it.
Omitted a description of a private LAN.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.3 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.2
```

2) Setting up the Virtual interface of IPv6

```
/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
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

4) 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
```

5) Setting up the Cluster configuration

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha1
```

6) Setting up the Wizard

To execute after completed "5) Setting up the Cluster configuration" in HOST-B.

7) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

[HOST-B]

1) Setting up the Virtual interface of IPv4

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.4 -t hme0,hme1
/opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.13.70.2
```

2) Setting up the Virtual interface of IPv6

```
/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
```

3) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

4) 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
```

5) Setting up the Cluster configuration

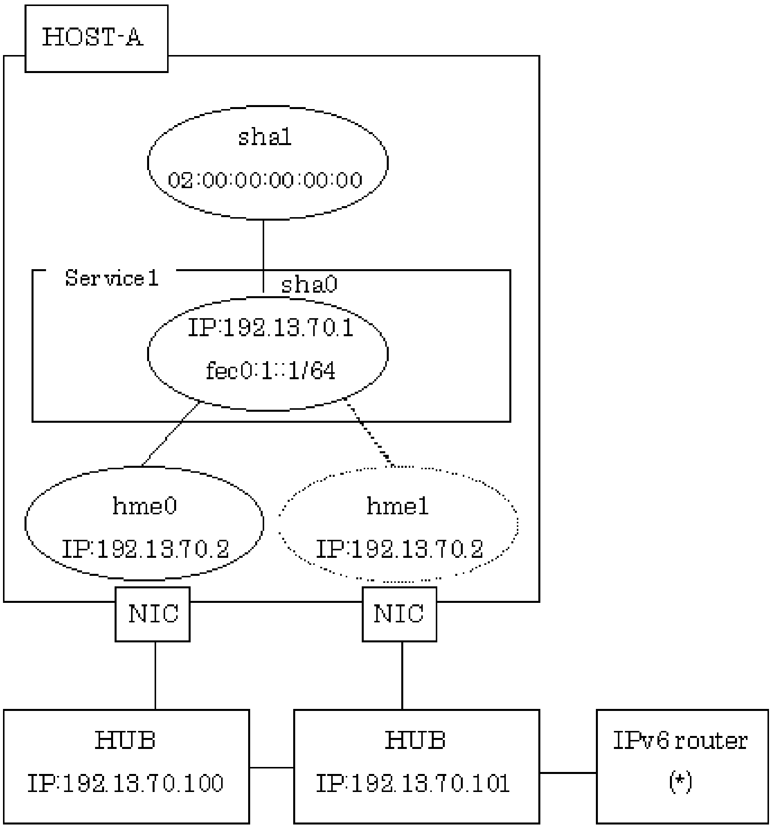
```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

6) Rebooting

When setting up of the HOST-A and HOST-B is complete, reboot both nodes simultaneously.

B.6.6 Example of the Cluster system (1 node cluster)

This section provides an example of setting up in the following network configuration.
If the Standby patrol monitoring function is not used, omit 3) in the procedure for setting up on each host.



(*) An example of setting /etc/inet/ndpd.conf when using a Solaris server as an IPv6 router is as follows:

```
ifdefault AdvSendAdvertisements on    # 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 Virtual interface of IPv4

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.13.70.1 -e 192.13.70.2 -t hme0,hme1

2) Setting up the Virtual interface of IPv6

/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t hme0,hme1

3) Setting up the HUB monitoring function

/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.13.70.100,192.13.70.101 -b on

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) Setting up the Cluster configuration

/opt/FJSVhanet/usr/sbin/hanethvrsc create n sha0

5) Setting up the Wizard

Set a wizard after completed to set cluster environment. It is not necessary to add a standby node (Machines[1]).

[Notes]
When setting a wizard from a node other than HOST-A in cluster environment configured by more than one node, set a HOST-A host name to an operation node (Machines[0]).

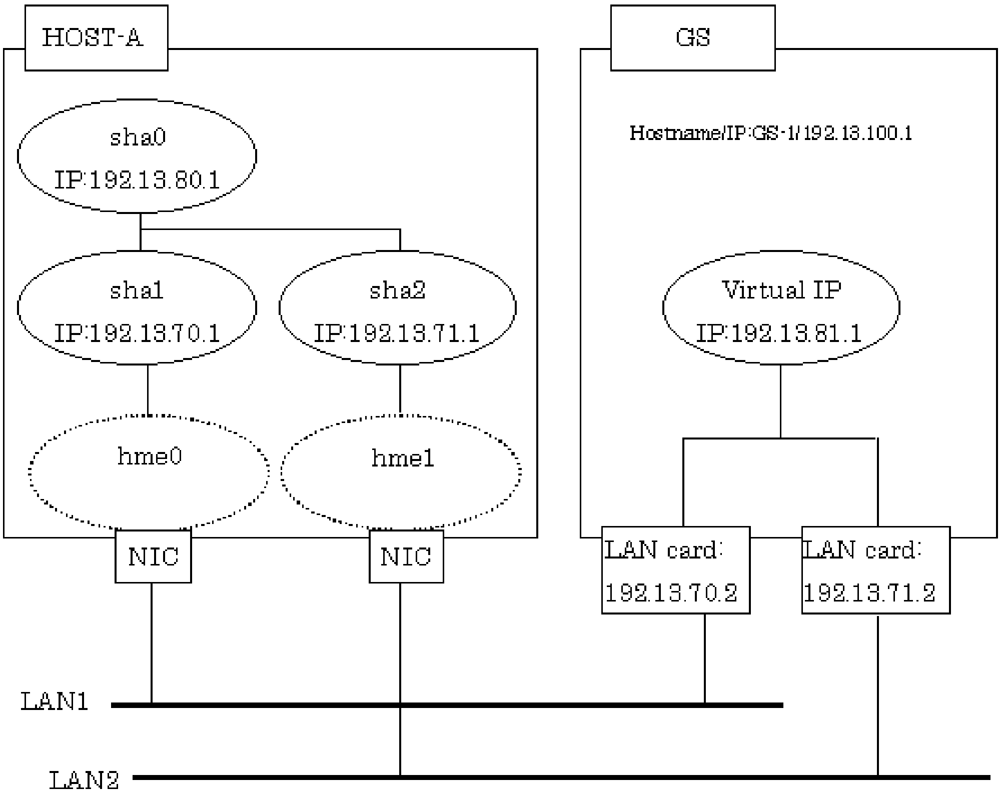
7) Rebooting

Reboot when completed all the environment setting.

B.7 Example of Setting up the GS/SURE linkage mode

B.7.1 Example of the Single system in GS communication function

This section provides an example of setting up in the following network configuration.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.13.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.13.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.13.80.1 -t sha1,sha2
```

2) Setting the Communication party monitoring function

An identifier of the monitoring information.

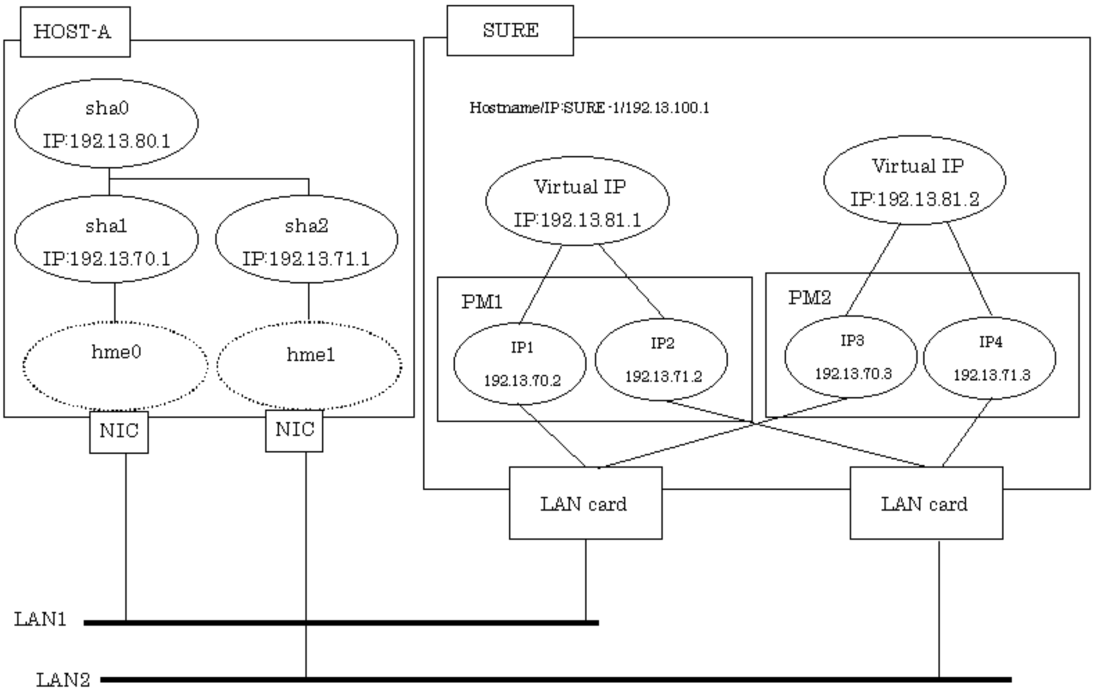
```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.13.81.1 -t 192.13.70.2,192.13.71.2 -m on
```

3) Rebooting

To reboot after completed the environment setting.

B.7.2 Example of the Single system in SURE communication function

This section provides an example of setting up in the following network configuration.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.13.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.13.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.13.80.1 -t sha1,sha2
```

2) Setting the Communication party monitoring function

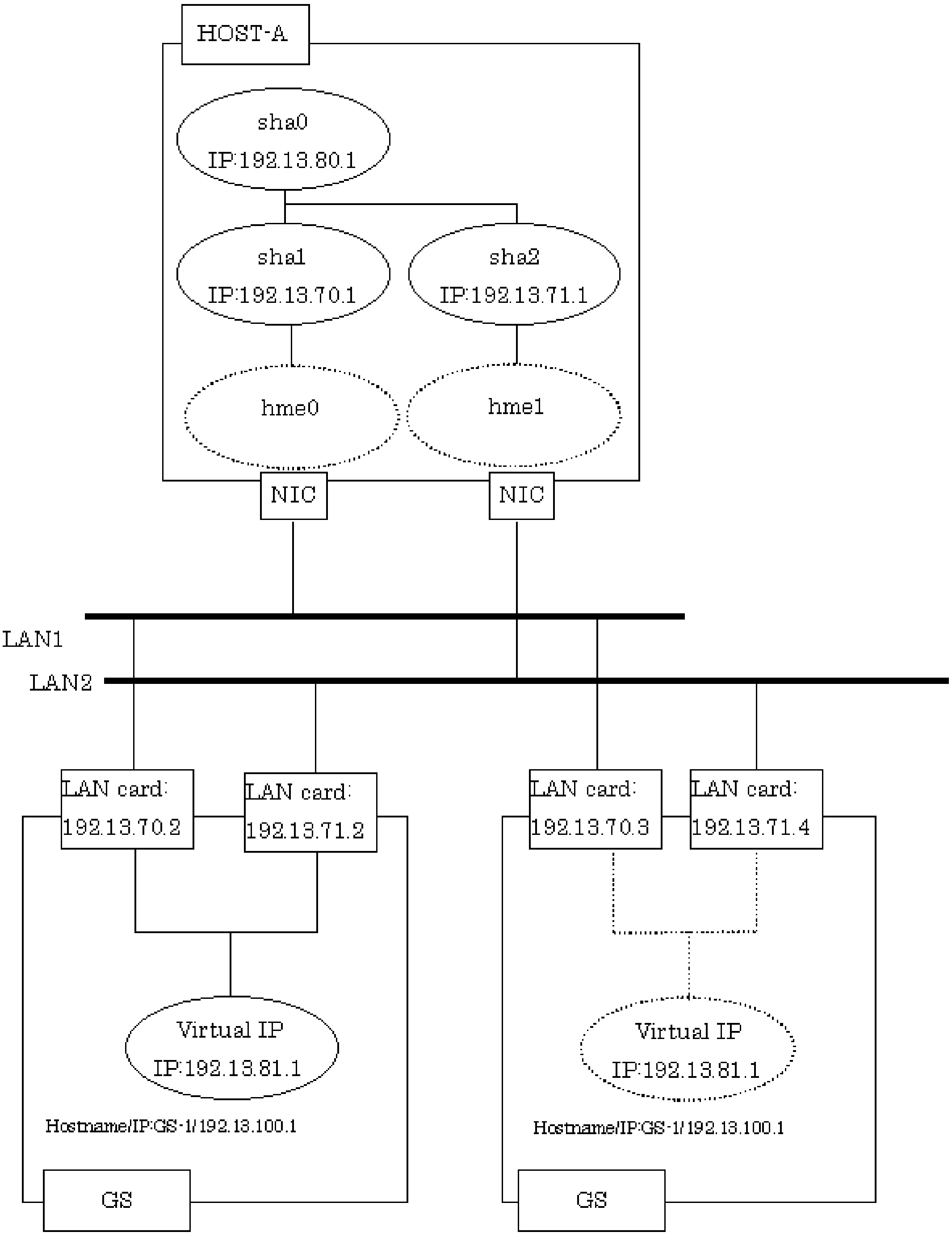
```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.13.81.1 -t 192.13.70.2:1,192.13.71.2:1 -m on
/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.13.81.2 -t 192.13.70.3:2,192.13.71.3:2 -m on
```

3) Rebooting

To reboot after completed the environment setting.

B.7.3 Example of the Single system in GS/SURE communication function

An example of the environment setting in a network configuration when the other system is a Hot standby system. The following configuration does not exist in SURE.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.13.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.13.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.13.80.1 -t sha1,sha2
```

2) Setting the Communication party monitoring function

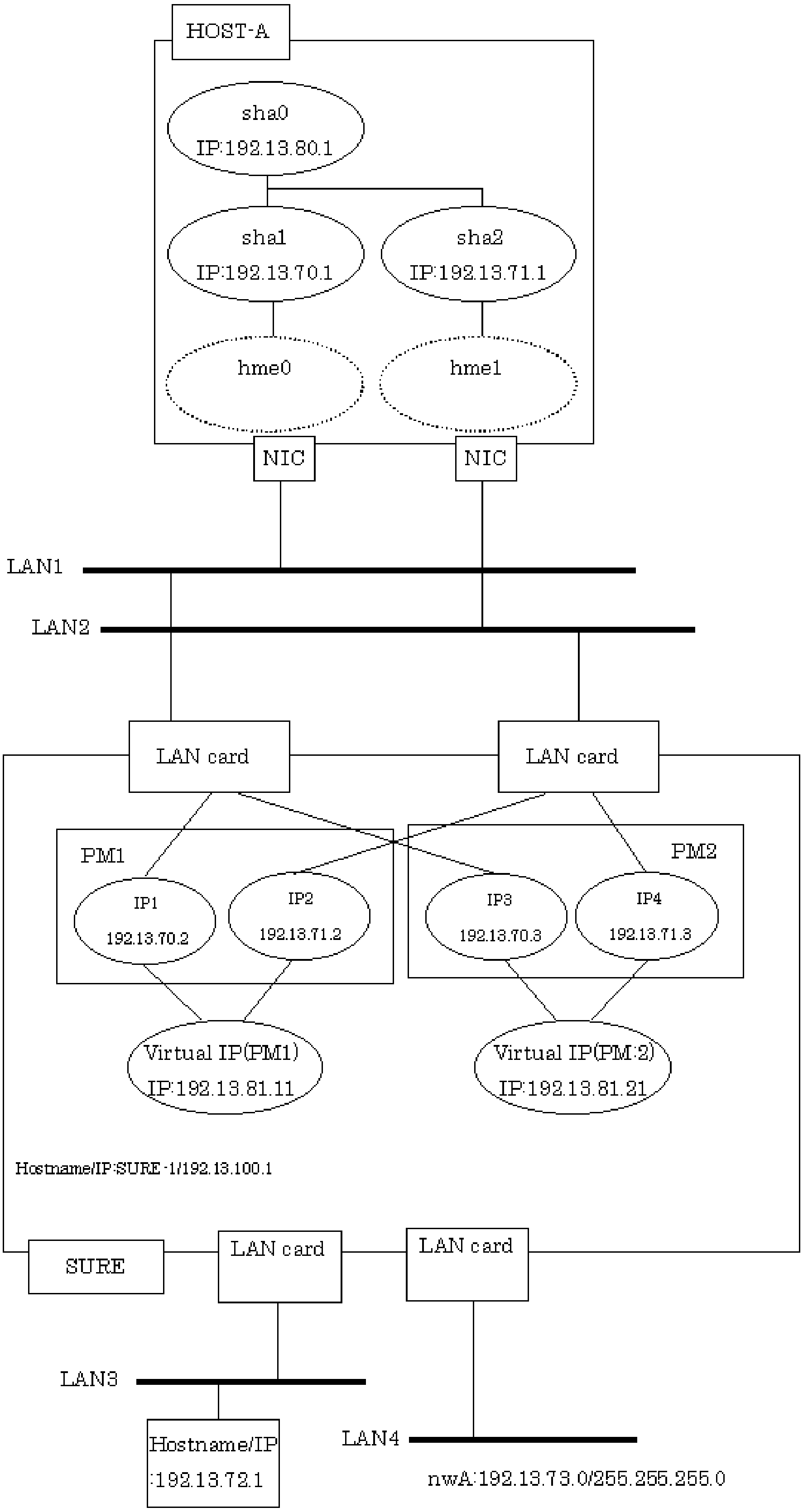
```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.13.81.1 -t 192.13.70.2,192.13.71.2 -m on
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.13.81.1 -t 192.13.70.3,192.13.71.4
```

3) Rebooting

To reboot after completed the environment setting.

B.7.4 Example of the Single system in TCP relay function

This section provides an example of setting up in the following network configuration.



[HOST-A]

1) Setting up the Virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.13.70.1 -t hme0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.13.71.1 -t hme1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.13.80.1 -t sha1,sha2
```

2) Setting the Communication party monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.13.81.1 -t 192.13.70.2:1,192.13.71.2:1 -m on
/opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.13.81.2 -t 192.13.70.3:2,192.13.71.3:2 -m on
```

3) Setting the relay destination information

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -i 192.13.81.1 -c 192.13.72.1,192.13.73.0:255.255.255.0
```

4) Rebooting

To reboot after completed the environment setting.

Appendix C Changes from old versions

None.

Appendix D Others

D.1 Changing Methods of Activating and Inactivating Interface

You must change the methods of activating and inactivating an interface to use such products as "INTERSTAGE Traffic Director" as a host application while Fast switching mode is used on a cluster system or NIC switching mode is used on a single system or a cluster system.

D.1.1 Fast switching mode

Execute the following command to use Fast switching mode. For more information on Section 7.6, "hanetparam Command".

```
# /opt/FJSVhanet/usr/sbin/hanetparam -t initialize
```

To stop the use of such products as "INTERSTAGE Traffic Director" and restore the methods of activating and inactivating an interface, execute the following command:

```
# /opt/FJSVhanet/usr/sbin/hanetparam -t cluster
```

D.1.2 NIC switching mode

Execute the following command to use NIC switching mode. For more information on Section 7.6, "hanetparam Command".

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d plumb
```

To stop the use of such products as "INTERSTAGE Traffic Director" and restore the methods of activating and inactivating an interface, execute the following command:

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d unplumb
```

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 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, not possible to set a default gateway. In a Redundant Line Control Function, a virtual interface is activated at activation of a service 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:

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, not possible to use a physical interface as a sending interface to a default gateway.

GS/SURE linkage mode:

Not possible to use a virtual interface as a sending interface to a default gateway in cluster operation.

D.2.2 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 service 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.2.3 Switching occurs even though no monitor-to device has an error in NIC switching mode

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, 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.

D.2.4 Takes time to execute an operation command or to activate a service

Phenomenon:

Takes time to execute an operation command of a Redundant Line Control Function.
Takes time to activate a service or to switch nodes at the cluster operation.

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.2.5 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.2.6 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:

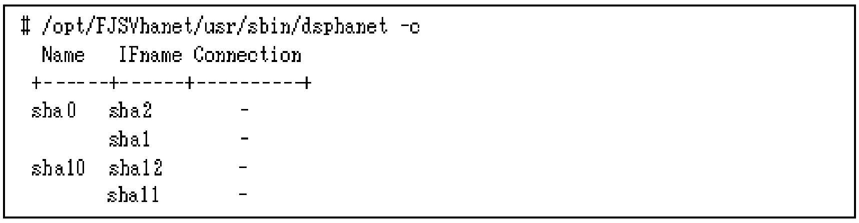
In a Redundant Line Control Function, when activating and deactivating an interface, or when detected an error in a transfer route, the route information is flushed and in.routed is reactivated if necessary. At this time, the static route information set by a route command is deleted.
When using in.routed, 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.2.7 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.2.8 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.2.9 Repeating switching in a node

Phenomenon:

In a cluster system, when detected an error in all of the redundant transfer routes, switching is repeated inside an operation node and takeover to a standby node is not done.

Cause and how to deal with:

When creating a cluster application (userApplication) of GLS (Global Link Services), there is a possibility that "AUTORECOVER(A)" is specified to an option parameter of a takeover IP address ("AdditionalTakeoverIpaddress"). In this case, change specification of an option parameter to "NOT:AUTORECOVER(N)".

See "The sub application Gls" of a Wizard manual for the detail.