PF6800 Ver. 6.0
Troubleshooting Guide

PFC00EK0600-01

Copyrights

Trademarks

Introduction

Thank you for purchasing the PF6800 (referred to as PFC). The PF6800 is a path control device used for centralized management of networks, and conforms to OpenFlow 1.0.

Unlike in conventional switch products, packet transfer and path control functions are separated, thus enabling greater flexibility in the network configuration.

To take full advantage of the functions of this product, please read this manual carefully and become fully familiar with the handling of this device.

About this Manual

This manual provides guidance on the method of diagnosis and replacement in times of faults in this product.

In the description, OFS refers to OpenFlow Switch and PFS refers to PF5xxx Switch.

In this manual, the PF5220, PF5240, and PF5248 are collectively referred to as the PF52xx.

The only OFS guaranteed to operate with this product is the NEC PFS.

Symbols

In this manual, the following three types of symbols are used. These symbols and their meanings are important for proper handling of the PFC.

Important

Indicates items for which special care should be taken to follow regarding handling of equipment and software operation.

Remember

Points that should be checked when operating devices or software.

Tip

Helpful, good-to-know information

Structure of this Manual

This manual includes five chapters. The following descriptions are provided in these chapters.

"Chapter 1. General Operation (page 1)"

Provides a summary of troubleshooting.

"Chapter 2. Troubleshooting Function Faults (page 4)"

Describes measures related to functional faults.

"Chapter 3. Procedure to Gather Information (page 34)"

Describes how to gather information for analysis.

Disclaimer

Unless explicitly set forth in a license agreement, NEC Corporation makes no explicit or implicit guarantees regarding this product and the related documentation, including its commercial use or fitness for a particular purpose, and disclaims all liability pertaining to its handling, use, or attendant trade practices.

Acknowledgment

We would like to express our thanks to Mr. Linus Torvalds and all the people involved in Linux development.

Contents

Chapter 1. General Operation

This chapter describes the general operation for fault analysis.

1.1 General Operation for Fault Analysis

Use this manual if there is a problem with the PF6800 series devices.

When checking the device by logging in, perform the analysis according to "1.2 General Operation for Functional Fault Analysis (page 1)".

1.2 General Operation for Functional Fault Analysis

The general operation for functional fault analysis for this device is shown in "Table 1-1 General Operation for Functional Fault Analysis (page 1)".

Table 1-1 General Operation for Functional Fault Analysis

Large Items	Medium Items	Reference Section
Trouble with the User Login	Cannot remember user password	"2.1.1 Cannot remember user password (page 4)"
	Cannot remember administrator (root) user password	"2.1.2 Cannot remember administrator (root) user password (page 4)"
Trouble with the Operable Terminal	It is difficult to login from the serial console.	"2.2.1 It is difficult to login from the serial console. (page 5)"
	Cannot remote login	"2.2.2 Cannot remote login (page 6)"
Control Network Failure	Cannot connect to the network	"2.3.1 Cannot connect to the network (page 7)"
	Cannot login to PFC Server	"2.3.2 Cannot login to PFC Server (page 8)"
	Cannot communicate with OFS by secure channel	"2.3.3 Cannot communicate with OFS by

Large Items	Medium Items	Reference Section
		secure channel (page 9)"
Virtual Network Failure	Checking station information	"2.4.1 Checking station information (page 10)"
	Failed in L2 network communication	"2.4.2 Failed in L2 network communication (page 10)"
	Failed in L3 network communication	"2.4.3 Failed in L3 network communication (page 11)"
	Cannot communicate using a flow filter	"2.4.4 Cannot communicate using a flow filter (page 12)"
	Cannot perform QoS-related control	"2.4.5 Cannot perform QoS-related control (page 13)"
	Failed in IPv6 communication	"2.4.6 Failed in IPv6 communication (page 14)"
	Trouble with broadcast communication	"2.4.7 Trouble with broadcast communication (page 15)"
	Topology detection failure	"2.4.8 Topology detection failure (page 18)"
	OFS transfer fails	"2.4.9 OFS transfer fails (page 19)"
	Communication is slow	"2.4.10 Communication is slow (page 20)"
	Packets do not flow when a new OFS or external terminal is connected	"2.4.11 Packets do not flow when a new OFS or external terminal is connected (page 21)"
	Cannot configure VLAN for OFS	"2.4.12 Cannot configure VLAN for OFS (page 21)"
	Alarms right after the start of the PFC server	"2.4.13 Alarms right after the

Large Items	Medium Items	Reference Section
		start of the PFC server (page 22)"
Cluster Trouble	Cluster does not run	"2.5.1 Cluster does not run (page 24)"
	Mirror disk data synchronization failure	"2.5.2 Mirror disk data synchronization failure (page 24)"
Trouble with Backup/Restore	A restore command was executed without specifying the -l option	"2.7 Trouble with Backup/ Restore (page 33)"
Others	-	Check the settings again by referring to the *Configuration Guide*.

Chapter 2. Troubleshooting Function Faults

This chapter describes how to troubleshoot when a functional failure occurs.

2.1 Trouble with the User Login

2.1.1 Cannot remember user password

If you have forgotten your user name or password for this device, login to the device as root user, and get the login user information. Ask the administrator with login privileges as root user to change the user information. For how to change user information, refer to *5.1 User Management* in the *Configuration Guide*.

2.1.2 Cannot remember administrator (root) user password

If you have forgotten the root user password for this device, disconnect the device from the cluster and restart it so that there is no effect on the network. The way to disconnect from the cluster is described in "4.1 Recovery Procedure upon Hardware/Software Replacement (page 35)".

Restart the device disconnected from the network in single user mode. The method to restart in single user mode is described below. Connect a display unit and keyboard to perform the following.

1. Restart the PFC in Single User Mode.
2. Change the Password.
3. Restart the PFC in Normal Mode.

2.1.2.1 Changing the password in single user mode

1. After switching OFF the PFC, switch it ON.
2. When `Press any key to continue.` is displayed upon PFC server startup, press any key.
3. When `Booting Red Hat Enterprise Linux…` is displayed, press any key again.
4. When the startup menu selection screen is displayed, select an item using the cursor keys and press the **E** key.
5. When the startup menu edit screen is displayed, use the cursor keys to move to the line starting with `kernel`, and then press the **E** key to edit the kernel startup options.
6. Specify `-s init=/bin/sh rw` in the startup options.

   When using the serial console, delete `console=tty0` and `rhgb` from the startup options.
7. Return to the previous screen by pressing the **Enter** key.
8. Press the **B** key, and when the PFC is booted, it runs in single user mode. It is possible to login to the PFC without a password in single user mode.
9. When the shell prompt is displayed, execute the following command to enable writing the file system.

   ```
   # mount o rw,remount /
   ```
10. Change the password by using the `passwd` command.

11. After the password has been successfully changed, reboot the PFC by using the `reboot` command.

2.1.2.2 Changing the password in rescue mode

1. Insert the PFC installation media in the DVD drive, turn off the PFC server, and then turn it on again.
2. The `PFC installation menu` is displayed. Select `Maintenance menu` using the cursor keys and press the **Enter** key.
3. The `Maintenance menu` is displayed. When you use a console, select `Rescue system` and press the **Enter** key. When you use a serial console, select `Rescue system(serial conso le)` and press the **Enter** key.
4. The message prompts you to insert the Red Hat Enterprise Linux 6.4 installation media. Press the **Enter** key.
5. When the language selection screen is displayed, select `English` using the cursor keys and press the **Enter** key.
6. On the keyboard layout selection screen, select `jp106` (for Japanese) using the cursor keys and press the **Enter** key.
7. On the Rescue Method selection screen, select `Local CD/DVD` using the cursor keys and press the **Enter** key.
8. On the Setup Network selection screen, select No using the **Tab** keys and press the **Enter** key.
9. On the Rescue selection screen, select `Continue` using the **Tab** keys and press the **Enter** key. On the following two or more confirmation screens, press the **Enter** key to proceed.
10. Finally, select `shell` and press the **Enter** key.
11. When the shell prompt is displayed, execute the following command to change the hard disk to the root directory.

```
# chroot /mnt/sysimage
```

12. Change the password by using the `passwd` command.
13. After the password has been successfully changed, return to the original root directory by using the exit command, and then restart the PFC server by using the `reboot` command. When the BIOS boot screen is displayed, remove the PFC installation media from the DVD drive.

2.2 Trouble with the Operable Terminal

2.2.1 It is difficult to login from the serial console.

If any connection trouble occurs with the serial console, check "Table 2-1 Connection Trouble with the Serial Console and Handling (page 5)".

Table 2-1 Connection Trouble with the Serial Console and Handling

Number	Fault Details	Details of Measures
1	Nothing is displayed on the screen.	Check the following. 1. Check that the cable is correctly connected.

Number	Fault Details	Details of Measures
		2. Check that the RS232-C cross cable is being used. 3. Check that the settings of the communication software, such as the port number, communication speed, data length, parity bit, stop bit, and flow control are as below. Communication speed: 9600 bps (setup value if changed) Data length: 8 bits Parity bit: none Stop bit: 1 bit Flow controls: none
2	Key input is not recognized.	Check the following. 1. It is possible that data communication on the flow controls is being interrupted by XON/XOFF. Stop the interruption of data communication (by pressing **CTRL**+**Q**). If key input is still not recognized, proceed to step 2. 2. Check that the settings are correct for the communication software. 3. The screen may have been stopped by pressing **CTRL**+**S**. Press any key.
3	When logging in, strange characters appear.	It is possible that the negotiation of the communication software is not correct. Refer to step 1, and set it correctly.
4	When entering user name, strange characters appear.	It is possible the communication speed of CONSOLE (RS232C) has been changed. Refer to step 1.
5	Cannot login	Check that the login prompt is displayed. If not, the device is being started. Wait until the device has finished starting up.
6	Strange symbols appear after changing the communication speed of the communication software after logging in, and it is not possible to enter commands.	After changing the communication speed of the communication software after logging in to the device, characters cannot be displayed normally. Return the communication speed of the communication software back to the original speed.
7	I want to login using the communication software, but when logging in, strange characters appear.	It is possible that the negotiation of the communication software is not correct. Refer to step 3. Try issuing a break signal. It may be necessary to issue multiple break signals to display the login screen depending on the communication speed of the communication software.
8	The item names and contents appear shifted	The displayed information may exceed the number of characters that can be displayed on one line. Change the screen size for the communication software, and increase the number of characters that can be displayed on one line.

2.2.2 Cannot remote login

If any connection trouble occurs with the remote operating terminal, check "Table 2-2 Connection Trouble with the Remote Operating Terminal and Handling (page 7)".

Table 2-2 Connection Trouble with the Remote Operating Terminal and Handling

Number	Fault Details	Details of Measures
1	Cannot remote connect	Check the following. 1. Check that a path is set up to remote connect using the `ping` command from the PFC. 2. If it takes time between displaying the connection setup message and displaying the prompt, it is possible that communication with the DNS server is not possible. (If communication with the DNS server is possible, it takes five minutes for the prompt to be displayed. Also, this time is an indication, and is different with each network.)
2	Cannot remotely connect after executing `Activate profile` by using the `pfc_netsetup` command.	Check that the remote connection destination is correct by using the following procedure. 1. If the IP address has been changed, specify the new IP address and then perform connection. 2. If connection fails after step 1, specify the IP address before the change and then perform connection. * If the `Activate profile` processing fails and an IP address is not allocated to the remotely connected interface, the network settings are rolled back to the status before `Activate profile` was executed.
3	Cannot login	Make sure that the user name and password are correct.
4	Key input is not recognized	Check the following. 1. It is possible that data communication on the flow controls is being interrupted by XON/XOFF. Stop the interruption of data communication (by pressing **CTRL**+**Q**). If key input is still not recognized, proceed to step 2. 2. Check that the settings are correct for the communication software. 3. The screen may have been stopped by pressing **CTRL**+**S**. Press any key.
5	There is a user logged in to the PFC shell.	Wait until the user is automatically logged out, or use the `killuser` command to delete any users that have logged in or are still logged in. Also, when editing the configuration, as it is still being edited and the configuration is not saved, after logging in again and saving in configuration mode, finish editing.

2.3 Control Network Failure

2.3.1 Cannot connect to the network

This device is equipped with three network interfaces with different purposes, the OpenFlow control network, operation network, and cluster interconnect network.

If it is thought that the cause of the communication failure is with the Ethernet port, check by executing the `ethtool` command.

1. Check the status of the Ethernet ports with the `ethtool` command.

```
pfcserver1:~ # ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
```

```
                            100baseT/Half 100baseT/Full
                            1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                            100baseT/Half 100baseT/Full
                            1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
```

2. Check the connectivity of the OpenFlow control network connecting the switch and the PFC server.

   Using the `ping` command on the standard PFC Server shell, check the network reachability of the switch. If there is no network reachability, check the control network settings and the cable connection status. As the OpenFlow control network is not controlled by OpenFlow protocol, check the cable connection status and packet loops, etc., in the same way as existing networks.

3. Check the PFC Server Hardware Status.

   Check the NIC status of the device. Run the PFC shell, and display the syslog information using the `show log syslog system` command. Check that there is a log for NIC in this log.

2.3.2 Cannot login to PFC Server

If it is not possible to login by ssh to the PFC Server from the OFS or an operating terminal, or if it is not possible to obtain a file from the PFC Server using the `scp` command, there are two possible points below.

1. The sshd on the appropriate PFC Server is not running.

   In this case, run the sshd on the appropriate PFC Server, and once again check the connection.

2. The settings of the authentication for sshd on appropriate PFC Server uses a public key system.

   In this case, check that the connecting terminal supports authentication using a public key cryptosystem. Access from terminals that do not support a public key cryptosystem will be denied. If accessing from a terminal that does not support a public key cryptosystem, it is necessary to login with only the password.

To check the settings for the sshd authentication system, it is possible to check from the file `/etc/ssh/ssh_config`.

```
# cat /etc/ssh/ssh_config
... Omission ...
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   GSSAPIDelegateCredentials no
#   BatchMode no)
```

Delete `#` (indicating that the line is a comment) from the underlined line to enable the setting.

2.3.3 Cannot communicate with OFS by secure channel

This device connects to OFS by a controlled communication path called secure channel. If there is a problem with the OpenFlow control network, it cannot connect the OFS, and OFS cannot be recognized by this device.

Run the CLI on this device, and check the status of the OFS by executing the `show ofs info` command in real-network mode.

```
PFC# cm real-network
[real-network]
PFC# show ofs info datapath-id 0000-0000-0000-0001 detail
Date: 2012-06-14 11:00:00 JST
OFS:DPID:0000-0000-0000-0001
  IP Address    :127.0.0.1
  Status        :connected
  AvoidStatus   :off
  Connected time:2011-03-03 08:30:30
  Connected for:0days 1hour 2minutes 30seconds
Port:  Name      :GBE0/1            ID:1
    … Omission …
```

The above execution example shows the case in which datapath-id of the OFS is 0000-0000-0000-0001.

If the results of the `show ofs info` command are not displayed, or `Status` is `disconnect` and communication by secure channel is not possible, the procedure for investigation is shown below.

1. Check the license.

   After the initial license has expired, it is not possible to connect to OFS without a valid license.

   Also, if the number of OFS instances specified by the license is not enough, the shortfall will not be able to connect to the OFS.

2. Check the OFS settings.

   The OFS is connected to the PFC via the secure channel. The PFC address must therefore be set to the OFS. In the PFC, set the IP address (floating IP in a cluster configuration) for the OpenFlow control network to the OFS. Refer to the *Configuration Guide* for the switch settings.

   Note that for an OFS in which datapath-id can be set, setting the same datapath-id in multiple OFSs may cause an unstable connection.

2.4 Virtual Network Failure

If a failure occurs in a virtual network, first check the following items.

- Check the configuration.

  If operation fails after adding new settings, check the configuration. The operating configuration can be checked by using the `show running configuration` command. Without executing the `commit` command after adding the `show running-configuration` command, the new setting is simply registered to the candidate configuration and is therefore not applied. If the PFC shell prompt display starts with `*`, there may be a candidate configuration that has not been committed.

- Check the alarm

The cause of path failure such as insufficient PFS resources or a broadcast distribution tree configuration failure can be identified by checking the alarm by using the `show alarm status` command.

- Operation check common to VTN

  If no alarm occurs but the packet transfer operation fails, identify the problematic part by performing an operation check common to VTN. For details about this operation check, refer to *4.1.3 Basic Steps to Check the VTN Operations* in the *Configuration Guide*.

The procedure for checking each function is described in the following sections.

2.4.1 Checking station information

When a packet reaches the virtual network from an external terminal, the terminal information is registered to the station database. Information including the station learning time, address, internal port, and mapped VTN name can be checked by referring to the station information.

```
PFC# show vtn-station
Date: 2012-06-14 11:48:00 JST
VTN station ID:271  Created time:2011-09-21 12:00:00
  MAC address:0012.e2d8.8cb8
  IP address :10.128.1.253
  OFS DPID   :0000-0000-0000-0121  PortName:GBE0/3  VLAN ID:3001
  MapType    :ofs-map  Status:valid
  VTN        :VTN1
  vExternal  :VEX1  Status:up
 ...
```

Possible execution results are shown below.

1. Station information from the terminal cannot be displayed, or expected values of the station information are different.

   Check the OSF setting, OFS connection, and VTN mapping.

2. Station information can be displayed correctly.

   Notwithstanding cases where the information from the appropriate terminal is displayed as expected, if communication is not possible, there is probably a problem with the VTN processing.

   Check and take measures as explained in the following sections.

2.4.2 Failed in L2 network communication

The procedure for checking a communication failure when vBridge is used within a virtual network is described below.

1. Check the reachability of the packet to vBridge.

   According to the operation check procedure common to all the VTNs (*4.1.3 Basic Steps to Check the VTN Operations* in the *Configuration Guide*), check whether the packet has reached each vBridge interface. If it has not, check that there is no problem in the topology to vBridge (vExternal and vlink connection) and the mapping settings.

2. Check the MAC address learning.

   Check that the packet has reached the vBridge virtual interface and its MAC address has been learned.

   Check that the value of the target interface of MAC learning is as expected by using the `show mac entry` command. In the case of a loop configuration with an external switch, the internal

port may change frequently. For example, storing two L2 switch ports when the STP is not operating in the same vbridge may result in a packet loop. In this case, check the network configuration and external switch settings. In addition, to secure a redundant path to the external L2 switch, use the link aggregation function of MCLAG or PF52xx.

show mac entry execution example

```
[vtn VTN1][vbridge BR1]
PFC# show mac entry
Date: 2012-06-14 11:48:20 JST
Mac Address          Type          Port          if-kind
0000.0000.0001      dynamic       BR1_1
0102.0304.0506      dynamic       BR1_2
ba98.7654.3210      dynamic       BR1_3*1
Total count: 3
```

*1 A terminal with the MAC address `ba:98:76:32:10` is connected to `Port BR1_3`.

2.4.3 Failed in L3 network communication

The procedure for checking a communication failure when vRouter is used within a virtual network is described below. For a failure that occurs during L3 communication via an external router, refer to "2.4.2 Failed in L2 network communication (page 10)".

1. Check the reachability of the packet to vRouter.

   According to the operation check procedure common to all the VTNs (*4.1.3 Basic Steps to Check the VTN Operations* in the *Configuration Guide*), check if the packet has reached each vRouter interface. If it has not, check that there is no problem in the topology to vRouter (vExternal, vBridge, and vlink connection) and the mapping settings.

2. Check the continuity to vRouter.

   Check the continuity between the terminal under vBridge connected to the vRouter and the vRouter by using the `ping` command. If ping fails, check that the IP address assigned to the vRouter interface is correct.

   show interface status execution example

```
[vtn vtn1][vrouter VRT1]
PFC# show interface status
Date: 2012-06-14 11:50:00 JST

Interface Information
InterfaceName:VIF_VRT1
 IfIndex:19
 AdminStatus:UP OperStatus:UP*1
 IpAddress:192.168.10.1 SubnetMask:255.255.255.0*1
 MAC Address:0225.5cca.0002 MTU:16000

InterfaceName:VIF_VRT2
 IfIndex:20
 AdminStatus:UP OperStatus:UP*1
 IpAddress:192.168.20.1 SubnetMask:255.255.255.0*1
 MAC Address:0225.5cca.0003 MTU:16000
```

   *1 Check that `AdminStatus` and `OperStatus` are `UP`, and that the `IpAddress/SubnetMask` values are as expected.

3. Check the routing settings.

Execute the `show ip route` command in the vrouter mode to display the IP routing information and check that a route to the communication destination IP network exists. If no route exists, set the routing information by using the `ip route` command. If the set route is incorrect, delete the setting by using the `no ip route` command, and then set it again.

show ip route execution example

```
[vtn vtn1][vrouter VRT1]
PFC# show ip route
Date: 2012-06-14 11:49:00 JST
Destination  Gateway    Genmask      Flags  Metric Use      Iface     NW
default    192.168.20.254  0.0.0.0    UGS    0         0      VIF_VRT2  N
192.168.10.0    *      255.255.255.0   U      0         0      VIF_VRT1  N
192.168.20.0    *      255.255.255.0   U      0         0      VIF_VRT2  N
```

4. Check the communication from the external router.

   vRouter does not support dynamic routing protocols including RIP. It is therefore impossible to exchange dynamic routing information with an external router by using a routing protocol. Set a static route to the vRouter network when using an external router if required.

2.4.4 Cannot communicate using a flow filter

The matching conditions for the packet filter and Policer functions are set by using the `flow-filter` command. If the traffic cannot be controlled as intended, check the statistics of the `flow-filter` command to identify the cause.

1. Check the statistics by using `show flow-filter`.

   Execute the `show flow-filter` command at the point where the filter is set to check the filter statistics and check whether hits with the intended matching conditions have been counted up.

   Execution example 1 (drop action)

```
 [vtn VTN0][vbridge BR13][interface R][filter in][sequence 1]
 PFC# show flow-filter
Date: 2012-04-01 16:20:57 JST
 flow-filter:in
 SeqNum   FlowList             Type      Action    NetworkMonitorGroup(status)
                                        Priority  DSCP
            SoftwarePacket ExistingFlowPacket ExpiredFlowPacket      TotalPacket*1
            SoftwareByte   ExistingFlowByte   ExpiredFlowByte        TotalByte*1
------------------------------------------------------------------------------
      1      all                   ip        drop      -
                                                 -     -
                     28                85                0             113*1
                   1718              9010                0           10728*1
```

   Execution example 2 (redirect action)

```
[vtn VTN1][vrouter VRT][interface RT3515]
PFC# show flow-filter in detail
Date: 2012-04-01 16:22:00 JST
flow-filter:in
SeqNum:1      TotalPacket(s):42840  TotalByte(s):4284000*1
                SoftwarePacket(s):0  SoftwareByte(s):0
                ExistingFlowPacket(s):42840  ExistingFlowByte(s):4284000
                ExpiredFlowPacket(s):0  ExpiredFlowByte(s):0
  FlowList:NM*1
    SeqNum:1*1
      TotalPacket(s):42840  TotalByte(s):4284000*1
        SoftwarePacket(s):0  SoftwareByte(s):0
        ExistingFlowPacket(s):42840  ExistingFlowByte(s):4284000
```

```
        ExpiredFlowPacket(s):0  ExpiredFlowByte(s):0
      Src IP:10.128.15.15/32
  Action:redirect
  RedirectDestination vNode:VEX3544_1  interface:VIF
modify-mac-destination:000c.29b4.22bf
  NetworkMonitorGroup:NM_BR3544
SeqNum:2      TotalPacket(s):0  TotalByte(s):0
                SoftwarePacket(s):0  SoftwareByte(s):0
                ExistingFlowPacket(s):0  ExistingFlowByte(s):0
                ExpiredFlowPacket(s):0  ExpiredFlowByte(s):0
  FlowList:NM
    SeqNum:1
      TotalPacket(s):0  TotalByte(s):0
        SoftwarePacket(s):0  SoftwareByte(s):0
        ExistingFlowPacket(s):0  ExistingFlowByte(s):0
        ExpiredFlowPacket(s):0  ExpiredFlowByte(s):0
      Src IP:10.128.15.15/32
  Action:redirect
  RedirectDestination vNode:VEX3546_1
interface:VIF modify-mac-destination:000c.296c.ad7d
  NetworkMonitorGroup:NM_BR3546
```

*1 Check the condition that matched (`SeqNum`) and transferred packet statistics.

2.4.5 Cannot perform QoS-related control

The Policer function can be used by PF52xx. For details about the PF52xx settings, refer to *3.2 OFS Setting* in the *Configuration Guide*.

For details on OFS setting errors, also refer to "2.4.9.2 The OFS flow table has been exhausted (page 19)".

When the Policer settings cannot be performed due to a PF52xx setting failure, etc., an alarm is displayed. Check that the following is not displayed as the execution result of the `show alarm status` command.

```
2012-04-27 11:29:58  warning  1620020000000606001
 occurred  VTN0
 Failure in a setup of Policer.
 ofs=0000-0000-0000-0126 port=3
 policer=VTN0
 policer_seqnum=1
```

In addition, whether the Policer function can be used with the connected PF52xx can be checked by using the `show ofs features` command.

Execution example of show ofs features detail for OFS with DPID=0000-0000-0000-0128

```
 PFC# show ofs features datapath-id 0000-0000-0000-0128 detail
Date: 2012-04-27 12:21:18 JST
OFS:DPID:0000-0000-0000-0128
  Status:connected
  Description:
    Manufacture:NEC Corporation
    Hardware   :PF5240F-48T4XW-A
    Software   :OS-F3PA Ver. V2.0.0.0
  Features:
    OpenFlow Switch Specification Version1.0.0:
      Action Enqueue
      Emergency
    Mirror
    Vendor:
      Drop Port
      Flow Strict
      IPv6
      L4 Port Filter
```

```
      MAC Address Filter
      Port Group
  Alarm:*1
    MPLS
      2012-04-27 10:57:28 VLAN connect
    Policer*1
      2012-04-27 11:29:58 CLI*1
```

*1 An alarm indicating the lack of a function because the Policer function is not supported is displayed.

Note that, even if the PF52xx supports the Policer function, you may fail in making the Policer settings like those above if the openflow-table-resource command is not correctly set. The mode value recommended for using QoS-related functions is 14.

```
PFS# show openflow resource
Date 2012/07/1 17:18:47 JST

FLOW tables resource information

  Table resource mode : 14

The remainder is omitted.
```

2.4.6 Failed in IPv6 communication

Whether the IPv6 matching function can be used with the connected PF52xx can be checked by using the `show ofs features` command. Check the functions supported by the OFS and the presence of an alarm indicating the lack of a function in the same way as in the execution example of the `show ofs features` command.

Execution example of show ofs features detail for OFS with DPID=0000-0000-0000-0128

```
 PFC# show ofs features datapath-id 0000-0000-0000-0128 detail
Date: 2012-04-27 12:21:18 JST
OFS:DPID:0000-0000-0000-0128
  Status:connected
  Description:
    Manufacture:NEC Corporation
    Hardware   :PF5240F-48T4XW-A
    Software   :OS-F3PA Ver. V2.0.0.0
  Features:*1
    OpenFlow Switch Specification Version1.0.0:
      Action Enqueue
      Emergency
    Mirror
    Vendor:
      Drop Port
      Flow Strict
      IPv6*1
      L4 Port Filter
      MAC Address Filter
      Port Group
  Alarm:
    MPLS
      2012-04-27 10:57:28 VLAN connect
    Policer
      2012-04-27 11:29:58 CLI
```

*1 This indicates that the IPv6 function is available.

2.4.7 Trouble with broadcast communication

The terminals may not communicate with each other, or the communication between them may be unstable due to a failure in broadcast or multicast communication of messages such as ARP and VRRP messages.

2.4.7.1 Check the topology (OFS core domain)

Broadcast and multicast traffics of the OFS core domain are transferred according to the distribution tree that connects the OpenFlow switches managed by this device. If the following message is displayed when checking for alarms by using the `show alarm status` command, the distribution tree cannot be built in the OFS core domain. Check whether the switch group is divided into two or more areas due to a link failure or wiring error in the OFS core domain, and recover the status. Check the OFSs that belong to the OFS core domain of the OFS domain and the OFS domain affiliation settings by using the `show ofs-domain`. If there is any error in the settings, correct the settings.

```
2013-05-09 18:15:41  warning  1490070000000134001
occurred
Broadcast OFS Core Domain Split
domain=DOMAIN1
```

Tip

If this alarm message is issued but the error is recovered immediately after the PFC server starts on the active or standby node, there is no problem.

2.4.7.2 Check the topology (OFS sub-domain)

Broadcast and multicast traffics of the OFS sub-domain are transferred according to the distribution tree that connects the OpenFlow switches managed by this device. Broadcast and multicast traffics between the distribution tree of the OFS sub-domain and distribution tree of the OFS core domain are transferred via the active port of the OFS sub-domain gateway.

If the following message is displayed when checking for alarms by using the `show alarm status` command, the distribution tree cannot be built in the OFS sub-domain or there is no active port in the OFS sub-domain gateway to connect to the distribution tree of the OFS sub-domain. Check whether the switch group is divided into two or more areas due to a link failure or wiring error in the OFS sub-domain and there is an active port in the OFS sub-domain gateway, and then recover the status. Check the OFSs that belong to the OFS sub-domain and the settings for the OFS domain affiliation and OFS sub-domain gateway by using the `show ofs-domain`. If there is any error in the settings, correct the settings.

```
2013-05-02 16:07:01  warning  1490080000000146001
occurred
Broadcast OFS Subdomain Split
domain=ofs_domain0001
subdomain=pfst_subdomain0001
```

Tip

If this alarm message is issued but the error is recovered immediately after the PFC server starts on the active or standby node, there is no problem.

Tip

When there are multiple distribution trees in one OFS sub-domain, it is also available to connect each distribution tree to the OSF core domain via an active port of the OFS sub-domain gateway.

2.4.7.3 Check the VLAN extended mode

When operating the PFC in the VLAN extended mode (`vlan-connect enable`), check the following.

Whether switches not supported for operation are connected

In the OFS core domain the VLAN extended mode, the PFS that can be used as an edge switch is the PF52xx of V3.0.0 or later. If PF52xx of V2.0.0 is used, the switch is disabled.

When using the PF1000 and PF54xx as an edge switch, they can be operated in the VLAN extended mode by using the OFS sub-domain configuration. For details, refer to *1.5.10 OFS Sub-Domain Function* in the *Configuration Guide*

The conflict status of `running-configuration` and the presence of switches that are not supported can be checked by using the `show vlan-connect` command. In the following example, the OFSs to be used as an edge switch with setting `vlan-connect` to `enable` do not support the required function (`Vendor:MPLS`). In this case, replace the OFSs with a switch that supports `Vendor:MPLS`.

Execution example of show vlan-connect

```
! PFC# show vlan-connect
Date: 2012-04-27 11:04:12 JST
current vlan-connect is enable.
check enable:No matching.*1
  0000-0000-0000-0001 does not support following features.*1
    Vendor:MPLS*1
  0000-0000-0000-0002 does not support following features.*1
    Vendor:MPLS*1
check disable:Matching OK.
```

*1 Shows the check result to `enable vlan-connect`.

2.4.7.4 Check the terminal location learning and DHCP packet settings

When using a redundant protocol such as HSRP in the external device connection or when performing IPv6 transfer, a PFC notification packet must be set.

Specify the settings according to *4.19 Setting Terminal Location Learning and DHCP Packets* in the *Configuration Guide*.

2.4.7.5 Check the MCLAG Settings

If a broadcast communication failure occurs while using MCLAG, check the stack link status.

stack link has a ring configuration, so it can operate normally if a single point of failure occurs, but cannot transfer packets if a double point of failure occurs. Check whether a double point of failure has occurred, and recover the failure status, if any.

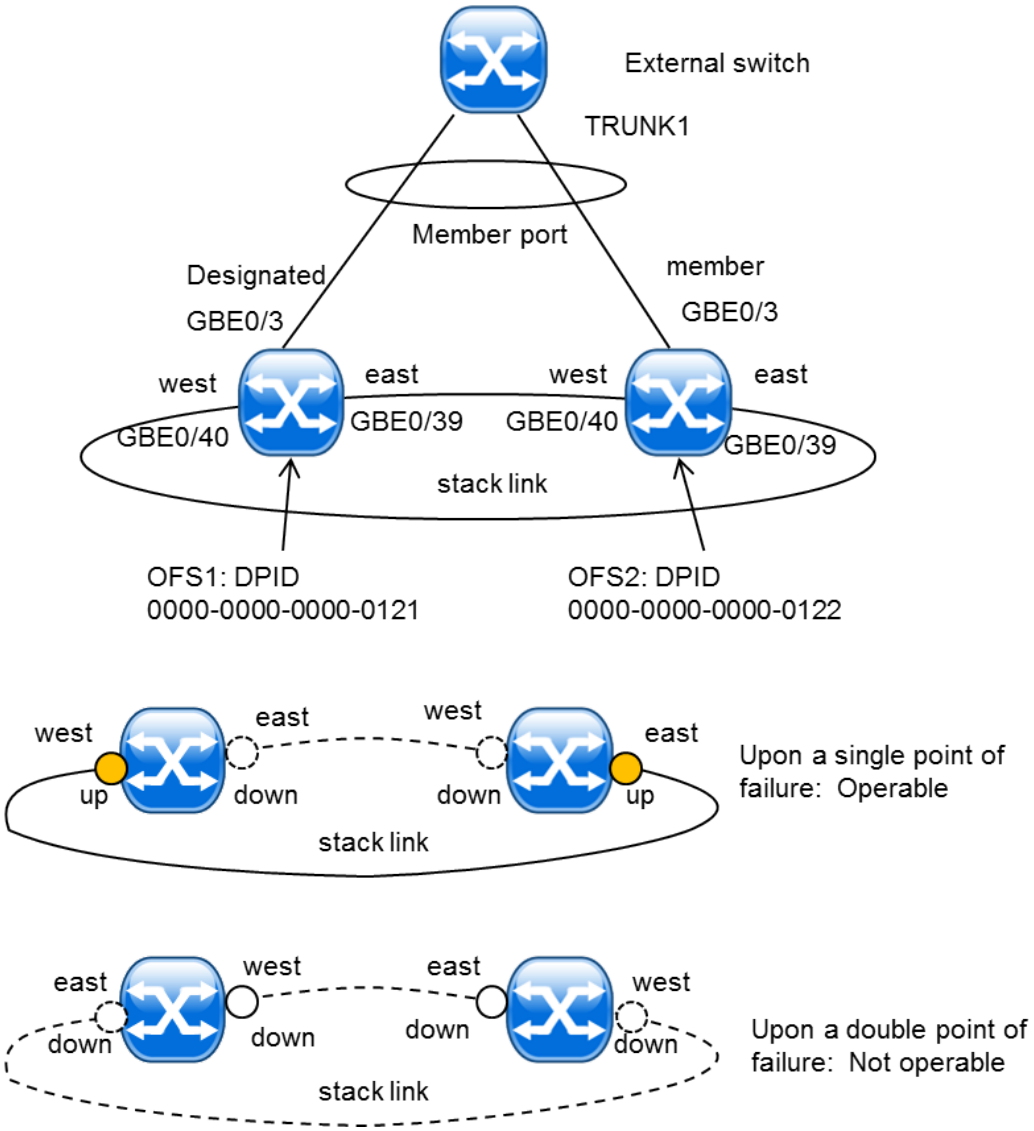

Figure 2-1 Whether Stack Link Is Operable When the Number of Member Ports Is 2

The stack link status can be checked with the show trunk-port command. The following shows an example of the status of a dedicated stack link. For details on the differences in the messages displayed by the dedicated stack link and those displayed by the shared stack link, refer to the *Command Reference*.

Execution example of show trunk-port upon double point of failure of stack link

```
[real-network]
    PFC# show trunk-port
Date: 2013-12-01 00:01:00 JST
TrunkName:TRUNK1
  Last designated time:2013-12-01 00:00:00
  Member ports:
    Member      OFSDPID              OFSPortName  Status
    designated  0000-0000-0000-0121  GBE0/3       up
    member      0000-0000-0000-0122  GBE0/3       up
  Stack link status:inactive*1
  Inactive stack link ports:*2
    OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/39
      Direction:east
      Status   :down
      Linked   :OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/40
                Direction:west
    OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/40
```

```
      Direction:west
      Status   :down
      Linked   :OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/39
                Direction:east
    OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/39
      Direction:east
      Status   :down
      Linked   :OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/40
                Direction:west
    OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/40
      Direction:west
      Status   :down
      Linked   :OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/39
                Direction:east
```

*1 If an inactive port exists, the `status` becomes `inactive`. If a setting error exists, the `status` becomes `error`.

*2 There are no active stack link ports, so the stack link is not operable.

Execution example of show trunk-port upon single point of failure of stack link

```
[real-network]
    PFC# show trunk-port
Date: 2013-12-01 00:01:00 JST
TrunkName:TRUNK1
  Last designated time:2013-12-01 00:00:00
  Member ports:
    Member      OFSDPID              OFSPortName  Status
    designated  0000-0000-0000-0121  GBE0/3       up
    member      0000-0000-0000-0122  GBE0/3       up
  Stack link status:inactive*1
  Active stack link ports:*1
    OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/40
      Direction:west
      Status   :up
      Linked   :OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/39
                Direction:east
    OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/39
      Direction:east
      Status   :up
      Linked   :OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/40
                Direction:west
  Inactive stack link ports:*2
    OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/39
      Direction:east
      Status   :down
      Linked   :OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/40
                Direction:west
    OFSDPID:0000-0000-0000-0122  OFSPortName:GBE0/40
      Direction:west
      Status   :down
      Linked   :OFSDPID:0000-0000-0000-0121  OFSPortName:GBE0/39
                Direction:east
```

*1 If there is an inactive port, the status becomes inactive. If there is a setting error, the status becomes error.

*2 When the number of member ports is 2, the stack link is operable if there is at least one pair of active stack link ports (east, west).

2.4.8 Topology detection failure

If communication fails in an environment in which external network devices such as an L2 switch and OFS are connected, check the following points.

Check the physical configuration by using the `show topology` command in real-network mode.

```
PFC# cm real-network
[real-network]
PFC#  show topology
OFS DPID:0000-0000-0000-0001
  Port:    Name: GBE0/1
    Neighbor:   OFS DPID:0000-0000-0000-0003  Port:GBE0/1
  Port:    Name: GBE0/2
    Neighbor:   OFS DPID:0000-0000-0000-0002  Port:GBE0/2
 ...
```

The example above shows the case when port GBE0/1 of an OFS with DPID: 0000-0000-0000-0001 is connected to port GBE0/1 of an OFS with DPID: 0000-0000-0000-0003. Check for setting errors, comparing the physical wire connection. If the destination DPID and port name are displayed in the `Neighbor` column while the OFS is connected to an external device, take any of the following actions.

- Stop topology detection by PLDP and fix the port as an external port by setting it as an external port according to *4.18 Setting Physical Network Direction* in the *Configuration Guide*.
- Check the LLDP setting of the external network device. If LLDP is set to the transparent mode, change the setting so that LLDP is blocked by a filtering function in the external network device, such as ACL. Note that the PLDP used by this device for topology detection has the same packet header as that of the LLDP supported by the external network device.

2.4.9 OFS transfer fails

2.4.9.1 No route exists

If is no valid route exists between the input and output switch ports in the communication flow, OFS transfer cannot be performed and transfer is performed via the PFC.

Check whether there is at least one candidate route that connects two OFSs by executing the `show path-candidate` command in real-network mode. The candidate routes are output by each PathPolicyIndex. Check the route policy information applicable for the target traffic. Note that the routes between the two OFSs may differ in direction. When checking the candidate communication routes between two OFSs (A and B), execute the command for each of the two combinations, (in-ofs, out-ofs) = (A, B) and (B, A).

If a candidate route is not displayed, there may be no route because the OFS is not wired correctly, or a link failure occurred. Check whether the OFS on the communication route is connected by executing the `show topology` command in real-network mode.

(Specify the datapath-id of the OFSs indicated by the underlined lines.)

```
 [real-network]
PFC# show path-candidate in-ofs datapath-id 0000-0000-0000-0121 out-ofs
 datapath-id 0000-0000-0000-0124
PathPolicyIndex:0
  PathInformation:
    Hop     InPort            OFS                  OutPort
    1                         0000-0000-0000-0121  GBE0/43
    2       GBE0/43           0000-0000-0000-0122  GBE0/44
    3       GBE0/44           0000-0000-0000-0124
```

2.4.9.2 The OFS flow table has been exhausted

When setting a flow to the OFS during virtual network processing, the flow setting may fail if the flow table within the OFS has been exhausted. If the flow setting fails, the flow uses PFC transfer,

resulting in a slower transfer rate. Check whether the flow table is full by using the `show alarm status` command.

In this case, the following message is output.

```
FlowEntry Full Occurred ofs=<value>
```

If this phenomenon occurs, review the network configuration and design. For example, setting detailed matching conditions for the flow filter may consume large part of the flow table.

The above alarm message is also output when the flow table used by the PFC does not exist within the OFS. For instance, it is output in the case that "openflow-table-resource mode" of the PF52xx is not set to use IPv6 in spite of setting the IPv6 matching condition to flow filter. Check the settings by using the `show running-config` command of the PF52xx, or check the Table resource mode by using the `show openflow resource` command and correct any error. The recommended value for PFC V3.0 is 14.

```
PFS# show openflow resource
Date 2012/07/1 17:18:47 JST

FLOW tables resource information

  Table resource mode : 14

… Omission …
```

2.4.10 Communication is slow

In the case of one-way communication of UDP traffic or test traffic where the MAC of the destination terminal has aged out, when the MAC address information of destination terminal ages out from the vBridge, communication is switched to broadcast communication known as Unknown Unicast at the vBridge (this is called flooding), resulting in slower communication. In addition, Unknown Unicast congests the secure channel and may affect other packet processing. Check whether Unknown Unicast has occurred by executing the `show status detail` command in vBridge mode.

```
[vtn VTN1][vbridge VBR1]
PFC# show status detail

vBridge    :VBR1                              Status :UP

 Interface :IF_VBR1_1                         Status :UP
RX:                                        TX:
 All:                                       All:
   Packets:                  0              Packets:                  0
   Octets :                  0              Octets :                  0
                                           Multicast/Broadcast:
                                             Packets:                  0
                                             Octets :                  0
                                           Unicast:
                                             Packets:                  0
                                             Octets :                  0

                                           Flooding:*1
                                             Packets:*1                0
                                             Octets :*1                0
                                           Host:
                                             Packets:                  0
                                             Octets :                  0
… Omission …
 Flooding:*2
  Unknown unicast:*2
   Count :*2                    0
```

```
 Multicast/Broadcast:*2
  Count :*2                    0

Drop:
 All:
  Packets:                   0
  Octets :                   0
 No route:
  Packets:                   0
```

*1 Counter for flooding that occurs in each interface.

*2 Counter for flooding that occurs at vBridge.

If this value has increased, Unknown Unicast has occurred.

To prevent this, run the ARP refresh function by using the `arp-agent enable` command in the vBridge. In addition, when Unknown Unicast occurs, limit the processing rate (number of original packets to be flooded per second) by executing the `unicast-flooding shaping-rate` command in real-network mode to prevent this problem affecting other packets.

For details about the `arp-agent enable` and `unicast-flooding shaping-rate` commands, refer to the *Command Reference* and *Configuration Guide*.

2.4.11 Packets do not flow when a new OFS or external terminal is connected

When a new OFS has been connected to the PFC or after a new external terminal is connected to an OFS, there may be occasions when packets do not flow.

Should this occur, use the `show alarm status` command to check whether alarm information like that shown below is displayed.

```
2012-09-11 14:44:16 warning 1500040000000114001
occurred
Default Flow Installation Failed
ofs=0001-0001-0001-0001
port=GBE0/12
```

If such information is displayed, the most likely cause is that the PFC has failed in initializing the OFS. In this case, execute the `audit ofs-port` command specifying the OFS and port in question. The above alarm is canceled when initialization is successful.

```
[real-network]
  PFC# audit ofs-port datapath-id 0001-0001-0001-0001 port GBE0/12
```

2.4.12 Cannot configure VLAN for OFS

When the automatic VLAN setting function is used, automatic setting may fail when a VLAN is configured.

In this case, use the `show alarm status` command to check whether alarm information like that shown below is displayed.

```
2012-11-06 17:53:28  warning  1810010000000109001
occurred
VLAN Misconfig Occurred
ofs=0001-0001-0001-0001
port=GBE0/12
```

Possible causes of this alarm are:

- The interface mode of the OFS port is set to access mode.
- When the port in question is an internal port, an untagged VLAN has already been configured for the OFS by the CLI (`switchport trunk native vlan` command) and its VLAN ID value is different from the PFC's default value (VLAN ID = 1) for the internal port.
- When the port in question is an external port, the untagged VLAN ID value set for the OFS is different from the untagged VLAN ID value set in ofs-map of the PFC.

Correct the error as described in *3.3 Enabling Automatic VLAN Setting* in the *Configuration Guide*, and then execute the `audit ofs-vlan` command. The alarm is canceled when the configuration is successful.

```
[real-network]
  PFC# audit ofs-vlan datapath-id 0001-0001-0001-0001 port GBE0/12
```

The `audit ofs-vlan` command may take time depending on the number of VLANs to be configured. Completion of the `audit ofs-vlan` command can be confirmed by checking operation logs.

```
Dec  4 10:00:00 pfc21 PFC.pfvlan: Starting VLAN audit of OFS 0000-0000-0000-0111.
Dec  4 10:00:05 pfc21 PFC.pfvlan: Finished VLAN audit of OFS 0000-0000-0000-0111.
```

If the automatic VLAN setting function is not used, check whether the VLAN is configured for the OFS, as described in *3.2 OFS Setup* in the *Configuration Guide*.

2.4.13 Alarms right after the start of the PFC server

Right after the PFC server starts, some types of alarms may occur temporarily. The alarms have risen in the time between the PFC server connects an OFS and it becomes available. This is not a problem, if these alarms recover after the PFC starts.

When an OFS get connected with the PFC, the alarms may occur and recover in the same way.

Among the alarms in question, the examples of alarms which severity is higher than warning level are shown below.

Table 2-3 Alarms that may be issued after the start of the PFC server

Type of Alarms	Explanation
OFS Port LinkDown	When an OFS get connected with the PFC, even if the status of ports of the OFS are link up, it seems that the status of the ports of it become link up from link down. If the automatic VLAN setting function is used, when a PF52xx is rebooted, the status of the ports has been link down until after the VLAN setting completes.
Physical Path Fault VTN Fault Broadcast Domain Split	These alarms can rise until the PFC recognizes the link connected between OFSs. Also the alarms can rise until the completion of the VLAN setting, if the automatic VLAN setting function is used.

If these alarms have corresponding operational log messages, the messages are output. However, these log messages do not mean problems if the corresponding alarms are restored.

Output example for OFS Port LinkDown

```
Dec  1 12:00:00 pfc21 PFC.pfcd[4346]: WARNING: libtm: Port is down. dpid=0000-0000-0000-0113,
port_name=10GBE0/50
```

Output example for Physical Path Fault

```
Dec  1 12:00:00 pfc21 PFC.pthctl: Path failed between OFS [0000-0000-0000-0111] and OFS [0000-
0000-0000-0113].
```

Output example for Broadcast Domain Split

```
Dec  1 12:00:00 pfc21 PFC.pthctl: Broadcast domain splits in [2] domains.(Centered OFS DPIDs:0
000-0000-0000-0111,0000-0000-0000-0112)
```

2.4.14 Confirming conduction of the path (Path OAM)

To troubleshoot a case where path conduction is not possible or desired multi-paths are not available even though there is a path between edge OFSs connected to the terminal and the physical link is valid, you can use the command "path-oam". This command can also be used to confirm whether there is a problem regarding path conduction after configuration change such as adding an OFS.

In the example below, confirm a path to another OFS from the OFS with datapath-id 0000-0000-0000-0001.

```
[real-network]
  PFC# path-oam in-ofs datapath-id 0000-0000-0000-0001 out-ofs all
```

Run the path-oam command, and then run the "show path-oam" command to confirm the result.

```
 [real-network]
  PFC# show path-oam
  IngressOFS           EgressOFS            Last Update          status
  -------------------  -------------------  -------------------  -----------
  0001-0000-0000-0001  0001-0000-0000-0004  2012-12-12 15:05:10  checking
  0001-0000-0000-0001  0001-0000-0000-0002  2012-12-10 14:29:34  active
  0001-0000-0000-0001  0001-0000-0000-0003  2012-12-09 20:28:16  fault
```

If "fault" is shown, conduction of at least one path has failed between the relevant OFSs. Add the "detail" option to show detail and confirm which link (between OFSs) is disconnected.

```
[real-network]
  PFC# show path-oam detail
IngressOFS: 0001-0000-0000-0001
  EgressOFS: 0001-0000-0000-0002  Status: active
    PolicyIndex:0
      MultipathID:0  Status: active
        Path info:
          Last Updated time: 2012-12-10 14:29:34
          SrcOFS               SrcPort  DstOFS               DstPort  time(msec)
          -------------------  -------  -------------------  -------  ----------
          0001-0000-0000-0001  GBE0/49  0001-0000-0000-0002  GBE0/17          30
      MultipathID:1  Status: active
        Path info:
          Last Updated time: 2012-12-10 14:29:30
          SrcOFS               SrcPort  DstOFS               DstPort  time(msec)
          -------------------  -------  -------------------  -------  ----------
          0001-0000-0000-0001  GBE0/48  0001-0000-0000-0002  GBE0/16          25
  EgressOFS: 0001-0000-0000-0003  Status: fault
    PolicyIndex:0
      MultipathID:0  Status: active
        Path info:
          Last Updated time: 2012-12-09 20:28:10
          SrcOFS               SrcPort  DstOFS               DstPort  time(msec)
          -------------------  -------  -------------------  -------  ----------
         0001-0000-0000-0001   GBE0/19  0001-0000-0000-0004  GBE0/18
         0001-0000-0000-0004   GBE0/16  0001-0000-0000-0003  GBE0/20          30
      MultipathID:1  Status: fault  Reason:timeout
        Path info:
          Last Updated time: 2012-12-09 20:28:15
          SrcOFS               SrcPort  DstOFS               DstPort  time(msec)
          -------------------  -------  -------------------  -------  ----------
          0001-0000-0000-0001  GBE0/20  0001-0000-0000-0005  GBE0/10          30
          0001-0000-0000-0005  GBE0/12  0001-0000-0000-0003  GBE0/14       *5000
  EgressOFS: 0001-0000-0000-0004  Status: checking
    PolicyIndex:0
      MultipathID:0  Status: checking
```

```
    Path info:
      Last Updated time: 2012-12-12 15:05:10
      SrcOFS               SrcPort   DstOFS               DstPort  time(msec)
      -------------------  -------   -------------------  -------  ----------
      0001-0000-0000-0001  GBE0/30   0001-0000-0000-0004  GBE0/35
  MultipathID:1  Status: checking
    Path info:
      Last Updated time:
      SrcOFS               SrcPort  DstOFS               DstPort      time(msec)
      -------------------  -------  -------------------  -----------  ----------
      0001-0000-0000-0001  GBE0/8   0001-0000-0000-0004  GBE0/9
```

If the result indicates failure, temporarily "avoid" the faulty OFS, conduct troubleshooting, replace equipment, and after releasing "avoid", run "path-oam" and confirm recovery.

2.5 Cluster Trouble

2.5.1 Cluster does not run

Check the cluster state by using the `pfc_show_cluster_status` command. If after executing this command, `Cluster not started.` is displayed, check that the following messages are not recorded in the syslog (`/var/log/messages`).

- syslog messages

```
Can't start PFC ClusterStateManager because CLUSTERPRO isn't running.
```

```
Can't start PFC ClusterStateManager because clpstat didn't become ready.
```

```
Can't start PFC ClusterStateManager because couldn't sync with CLUSTERPRO.
```

```
pfccsmd abnormally terminated.
```

If the above messages are recorded in the syslog, the PFC cluster is not properly running. Check the other messages in the syslog, and resolve the cause of the problem.

As the PFC cluster is based on CLUSTERPRO, a problem has occurred with the resources of CLUSTERPRO, and it is not possible to start the cluster. In this case, it is necessary to resolve the problem with CLUSTERPRO. The next chapter explains the recovery method when a mirror break has occurred on the mirror disk resources of CLUSTERPRO.

2.5.2 Mirror disk data synchronization failure

A PFC updated from a version lower than V3.0.0 uses a mirror disk to share data between cluster nodes. A mirror break is the status when the data of the mirror disk, which is used for sharing data between the cluster nodes, is not synchronized. A mirror break is usually caused by the following.

- PFC on a redundant configuration is launched with a time difference of more than five minutes
- PFC on a redundant configuration is operated with a single configuration
- A network partition has occurred on the PFC cluster
- PFC is stopped unintentionally such as in a power outage

Refer to *Chapter 6 "PFC Redundancy Setup"* in the *Configuration Guide* for precautions relating to operating a cluster when there is a network partition or mirror break on the PFC cluster. Below is an explanation of troubleshooting when there is a mirror break.

In this section, CLUSTERPRO commands are used to recover from a mirror break. A list of the CLUSTERPRO commands used is shown below.

Table 2-4 CLUSTERPRO Commands

Command	Function / Usage	
`clpmdstat`	Function	Displays mirror disk status
	Usage	Checks mirror break status
`clpmdctrl`	Function	Mirror disk resource operation
	Usage	Recovers mirror brake status
`clpcl`	Function	Cluster operation
	Usage	Starts the cluster manually
`clpmonctrl`	Function	Monitor resource operation
	Usage	Suppresses monitoring of resources not started when running a cluster manually.

The major errors output by each command are shown below. If a message prompting disk replacement or any message other than those shown below is output, contact the maintenance and service company.

Table 2-5 Major Error Messages

Command Name		
Error Message		**Cause and Action**
`clpmdstat`	Error: Log in as root.	Execute as a root user.
	Error: Failed to acquire the active status of the Mirror Agent of the local server. Shut down the cluster and reboot both servers	Failed to acquire the active status of the local server mirror disk resource. Shut down the cluster and then reboot both servers.
	Error: Failed to acquire the active status of the Mirror Agent of the other server. Shut down the cluster and reboot both servers	Failed to acquire the active status of the other server mirror disk resource. Shut down the cluster and then reboot both servers.
	Error: Failed to acquire mirror recovery status. Reboot the local server.	Failed to acquire the mirror recovery status. Reboot the local server.
	Error: Failed to acquire the list of mirror disks. Reboot the local server.	Failed to acquire the mirror disk list. Reboot the local server.
	Error: The number of the bits of the bitmap is invalid. The mirror difference information of the cluster partition is invalid. Shut down the cluster. If it fails again, replace the disk. For procedure to replace the disk, see the Reference Guide.	Failed to acquire the mirror difference information of the cluster partition. Shut down the cluster. If this error occurs again, replace the disk.
	Error: Failed to get bitmap information. Failed to acquire the mirror difference information of the local server. Reboot the local server.	The mirror difference information of the cluster partition is invalid. Shut down the cluster. If this error occurs again, replace the disk.

Command Name		
Error Message		**Cause and Action**
	Error: Failed to read the mirror difference information of the local server. Reboot the local server.	Failed to read the mirror difference information of the local server. Reboot the local server.
	Error: Failed to acquire semaphore. Reboot the local server.	Failed to acquire a semaphore. Reboot the local server.
	Error: A malloc error. Failed to reserve the memory space. Reboot the local server.	Failed to reserve memory space. Reboot the local server.
	Error: Internal error (errorcode: 0xxxx). Shut down the cluster and reboot the server.	Shut down the cluster and then reboot the server.
	Error: Failed to acquire the mirror disk detail information of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire detailed information of mirror disks of both servers. Shutdown the cluster and then reboot the both servers. %1 and %2 are replaced with server names.
	Error: Failed to acquire mirror disk %3 net interface status of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire mirror disk connection status of both servers. Shut down the cluster and then reboot both servers. %1 and %2 are replaced with server names. %3 is replaced with the mirror resource name.
	Error: Failed to acquire the active status of the Mirror disk %3 of the server %1 and server %2. Shut down the cluster and reboot both servers.	Failed to acquire the mirror disk resource status of both servers. Shut down the cluster and then reboot both servers. %1 and %2 are replaced with server names. %3 is replaced with the mirror resource name.
`clpmdctrl`	Error: Log in as root.	Execute as a root user.
	Error: A hardware error has occurred on the disk. Check the disk.	A hardware error occurred on the disk. Check the disk.
	Error: Specification of the server that is copied from is incorrect. When executing mirror recovery again after a failure end of mirror recovery, specify the same server as the previous one.	The specification of the copy source server is incorrect. When executing mirror recovery again after mirror recovery is terminated by an error, specify the same copy source server as the previous one.
	Error: Forced mirror recovery is required. Run the clpmdctrl -force command to perform the recovery.	Forced mirror recovery is required. Run the `clpmdctrl --force` command to perform recovery.
	Error: Server with old data is specified as the server which is copied from. Specify a correct recovery direction.	A server with old data is specified as the copy source serves. Specify the correct recovery direction.
	Error: Failed to acquire mirror recovery status. Reboot the local server.	Failed to acquire the mirror recovery status. Reboot the local server.
	Error: Failed to acquire the mirror disk configuration information. Reboot the local server.	Failed to acquire the mirror disk setting information. Reboot the local server.

Command Name		
Error Message		**Cause and Action**
	Error: Failed to acquire the mirror disk configuration information of both local and remote servers. Shut down the cluster and reboot both servers	Failed to acquire the mirror disk setting information of both servers. Shut down the cluster and then reboot both servers.
	Error: Failed to read the mirror difference information of the local server. Reboot the local server.	Failed to read the mirror difference information of the local server. Reboot the local server.
	Error: Failed to read the mirror difference information of the other server. Reboot the other server.	Failed to read the mirror difference information of the other server. Reboot the other server.
	Error: Failed to get the bitmap information of the local server due to the errors occurred when acquiring the mirror difference information of the local server. Reboot the local server.	Failed to read the mirror difference information of the local server. Reboot the local server.
	Error: Failed to read the disk space. Shut down the cluster and reboot the server	Failed to acquire the disk space information. Shut down the cluster and then reboot the server.
	Error: Failed to acquire the disk space of the other server. Shut down the cluster and reboot both servers.	Failed to acquire the disk space information of the other server. Shut down the cluster and then reboot the server.
	Error: Error occurred on the settings of the mirror disk resource. Reboot the local server.	An error occurred in the mirror disk resource status setting. Reboot the local server.
	Error: Failed to create a thread. Reboot the local server.	Failed to create a thread. Reboot the local server.
	Error: Internal error. Failed to create process. Reboot the local server.	Failed to create a process. Reboot the local server.
	Error: Failed to acquire semaphore. Reboot the local server.	Failed to acquire a semaphore. Reboot the local server.
	Error: A malloc error. Failed to reserve the memory space. Reboot the local server.	Failed to reserve memory space. Reboot the local server.
`clpcl`	Error: Log in as root.	Execute as a root user.
	Performed startup processing to the active cluster daemon.	Startup processing was executed on an active CLUSTERPRO daemon.
	Server is busy. Check if this command is already run.	This command may already be running. Check the status.
	Internal error. Check if memory or OS resources are sufficient.	The memory or OS resources may be insufficient. Check the status.
`clpmonctrl`	Log in as root.	Cannot execute the command with your user privilege. Execute as a root user.
	Initialization error. Check if memory or OS resources are sufficient.	The memory or OS resources may be insufficient. Check the status.

Command Name		
Error Message		**Cause and Action**
	This command is already run.	The command is already running. Check the execution status by using commands such as ps.
	Internal error. Check if memory or OS resources are sufficient.	The memory or OS resources may be insufficient. Check the status.

2.5.2.1 How to check mirror break status by using commands

Check mirror break status by using the commands below.

```
# clpmdstat -mirror md1
```

The status of the mirror disk resources is displayed by executing the `clpmdstat` command.

- When normal (Mirror Color are all GREEN)

```
Mirror Status: Normal

md1             server1    server2
-----------------------------------------------------------
Mirror Color    GREEN      GREEN
```

- When mirrors need recovery (any Mirror Color is RED)

```
Mirror Status: Abnormal
Total Difference: 1%

md1                server1                  server2
-----------------------------------------------------------
Mirror Color       GREEN                    RED
Lastupdate Time    2011/03/04   17:30:05    --
Break Time         2011/03/04   17:30:05    --
Disk Error         OK                       OK
Difference Percent 1%                       --
```

  Recover the mirror disk by referring to "2.5.2.3 How to recover a mirror by using commands (page 29)".

- When mirrors need forced recovery (`Mirror Color` is all `RED`)

```
Mirror Status: Abnormal
Total Difference: 1%

md1                server1              server2
-----------------------------------------------------------
Mirror Color       RED                  RED
Lastupdate Time    2011/03/09 14:07:10  2011/03/09 13:41:34
Break Time         2011/03/09 14:06:21  2011/03/09 13:41:34
Disk Error         OK                   OK
Difference Percent 1%                   1%
```

  Recover the mirror disk by referring to "2.5.2.4 How to force recover a mirror by using commands (page 29)".

- When in the middle of processing of a mirror recovery

  Recover the mirror disk by referring to "2.5.2.2 How to check execution status during a mirror recovery by using commands (page 29)".

2.5.2.2 How to check execution status during a mirror recovery by using commands

Check execution status of processing of a mirror recovery by using the commands below.

```
# clpmdstat --mirror md1
```

- During the processing of a mirror recovery the following information is displayed.

```
Mirror Status: Recovering

md1                server1         server2
-------------------------------------------------
Mirror Color       YELLOW          YELLOW

Recovery Status    Value
--------------------------------------
Status:            Recovering
Direction:  src    server1
            dst    server2
Percent:           7%
Used Time:         00:00:09
Remain Time:       00:01:59
Iteration Times:   No Limit
```

- When the processing of a mirror recovery is completed the following information is displayed.

```
Mirror Status: Normal

md1              server1     server2
-----------------------------------------------------------
Mirror Color     GREEN       GREEN
```

2.5.2.3 How to recover a mirror by using commands

By executing the command below on any server on the cluster, mirror recovery will begin.

```
# clpmdctrl --recovery md1
```

When differential mirror recovery is possible, recovery will be conducted using differential information. In the case of a differential mirror recovery, recovery time will be reduced.

With this command, when the mirror recovery is executed, the controls return straight away. See "2.5.2.2 How to check execution status during a mirror recovery by using commands (page 29)" for details about the status of the mirror recovery.

However, if the `Mirror Color` of the mirror disk on an active node is `RED`, executing the above command will result in an error and the mirror cannot be recovered. Force mirror recovery by executing the following commands on the server of a standby node.

```
# clpmdctrl --break md1
# clpmdctrl --force <active node server name> md1
```

2.5.2.4 How to force recover a mirror by using commands

When it is not possible to determine which server on CLUSTERPRO is storing new data, a force mirror recovery is necessary.

In cases like this, it is necessary to manually specify the server storing store new data, and force mirror recovery. In forced mirror recovery, it will take significantly longer to complete recovery compared to a differential mirror recovery as it is a full copy.

1. Specify the server storing new data

   Specify the server holding new data based on information leading the time and occurrence of the mirror break as below.

   - Check by using the `clpmdstat` command

     a. Execute the following command:

     ```
     # clpmdstat --mirror md1
     ```

     b. Check the last time data was updated (`Lastupdate Time`), and specify the server holding new data. However, the time of the last update of data depends on the time set on the OS.

   - Determining from the failure history

     If a network partition has occurred, the server which was originally running on standby may become the newest. In cases like this, it is probably best to set a server that was originally operating as an active node as the server to hold new data.

   - Determining from the operating history

     If the commands `save configuration`, `import startup-configuration <FILE >`, or `commit` have been executed in the PFC Shell, when the user management information is changed as an operation on the GUI, or the position of icons, background color, or background map on the physical or VTN topology map are changed, or when the settings relating to sFlow are changed, the data is synchronized between the servers in the redundant configuration. If these operations are performed before or after a mirror disk is generated, the data may not be synchronized between servers on a redundant configuration, but stored only on the server where the operation was performed. If the server storing required data (through performing the operation) is clear, set the server storing the required data as the server to store new data, regardless of the time of update.

     Tip

     Refer to *6.5 Precautions Related to Cluster Operation* in the *Configuration Guide* for precautions related to network partitions.

2. Forcibly recover the mirror

   If it is possible to specify the server storing new data, forcibly recover the mirror by executing the commands below on any server on the cluster.

   ```
   # clpmdctrl --force <Name of server storing new data> md1
   ```

   The `clpmdctrl` command is not limited to when the force mirror recovery is complete in order to quickly return the controls when a force recovery has started. See "2.5.2.2 How to check execution status during a mirror recovery by using commands (page 29)" for details about the status of the force mirror recovery.

   However, when the cluster is operating with only 1 node, it is not possible to force a mirror recovery. After executing the above command, if the `Mirror Color` is `YELLOW` or `GREEN` when checking the condition of the mirror recovery, check the cluster status by using the `pfc_show_cluster_status` command. If the cluster has stopped on only one of the servers, manually run the cluster on the server where the cluster has stopped by using the command below, and force a mirror recovery.

   ```
   # clpcl -s ; sleep 30 ; clpmonctrl -s
   ```

If the cluster has stopped on all servers joining a redundant configuration, it is not necessary to manually run the cluster, as a force mirror recovery is possible in this state.

After confirming completion of the force mirror recovery, it is possible to use the mirror disk. If the cluster is running before operating a force mirror recovery, after the force mirror recovery is complete, reboot the server.

2.5.2.5 How to force recover a mirror on a single server by using commands

Sometimes a server may be unable to run due to a hardware or OS failure, and it is not guaranteed that new data will be stored on a server which can run.

When wishing to start work only on a server which can run, it is possible to force a mirror recovery on the server which can run.

By executing this operation, the server on which the command was executed will be forced to store new data. For this reason, if the server which could not run is able to run, the data on the server on which the force mirror recovery was performed will be copied, and the originally stored data cannot be used.

From what we have understood so far, manually execute the command below.

By executing the command below, the force mirror recovery will begin.

```
# clpmdctrl --force md1
```

After executing the command, it is possible to use the mirror disk.

Furthermore, to replace a server which is unable to run, refer to "Chapter 4. Procedure for Replacement (page 35)" explaining the procedure for rebuilding a cluster.

2.6 Dual Cluster Trouble

2.6.1 Automatic backup/Main cluster operation status cannot be acquired

1. Confirm that the FIP address of the management network connection interface of main cluster is properly registered in reserve cluster.

   Run the following command on active and standby PFC servers of reserve cluster to confirm. If FIP address is not registered properly, redo the FIP address registering procedure.

```
# pfc_dual_cluster -s
Dual-Cluster position: reserve
Dual-Cluster function: enabled
Opposite cluster IP address (FIP): 10.0.0.11
Opposite cluster IP address (1): 10.0.0.1
Opposite cluster IP address (2): 10.0.0.2
Secure Channel TCP port: 6633
```

Tip

In execution example above, the place in bold is checkpoint, and the IP address is an example.

Tip

About FIP address registering procedure, refer to *7.4.1 Enabling the Dual Cluster Function7.4.1.3 Setting of the Reserve Cluster (2)* in *Configuration Guide*

2. Confirm that public and private keys are distributed in appointed location in active and standby PFC servers of reserve cluster.

   Run the following command on active and standby PFC servers of reserve cluster to confirm. If public and private keys are not distributed properly, redo the key distributing procedure.

```
# ls /root/.ssh/pfc_dual_cluster_id_rsa
/root/.ssh/pfc_dual_cluster_id_rsa
# ls /root/.ssh/pfc_dual_cluster_id_rsa.pub
/root/.ssh/pfc_dual_cluster_id_rsa.pub
```

Tip

In execution example above, the place in bold is checkpoint.

Tip

About public and private keys distributing procedure, refer to *7.4.1 Enabling the Dual Cluster Function7.4.1.1 Setting of the Reserve Cluster (1)* in *Configuration Guide*

3. Confirm that public and private keys are distributed in appointed location in active and standby PFC servers of main cluster.

   Run the following command on active and standby PFC servers of main cluster to confirm. If public and private keys are not distributed properly, redo the key distributing procedure.

```
# ls /root/.ssh/pfc_dual_cluster_id_rsa
/root/.ssh/pfc_dual_cluster_id_rsa
# ls /root/.ssh/pfc_dual_cluster_id_rsa.pub
/root/.ssh/pfc_dual_cluster_id_rsa.pub
```

Tip

In execution example above, the place in bold is checkpoint.

Tip

About public and private keys distributing procedure, refer to *7.4.1 Enabling the Dual Cluster Function7.4.1.2 Setting of the Main Cluster* in *Configuration Guide*

2.6.2 Cannot be switched from main cluster to reserve cluster

1. Check that the switchover command (pfc_dual_cluster --switchover) is executed in the active PFC server (with Dual Cluster Function enabled) of reserve cluster.

   Run the following command to confirm.

```
# pfc_dual_cluster -s
Dual-Cluster position: reserve
Dual-Cluster function: enabled
Opposite cluster IP address (FIP): 10.0.0.11
Opposite cluster IP address (1): 10.0.0.1
Opposite cluster IP address (2): 10.0.0.2
Secure Channel TCP port: 6633
```

```
# pfc_show_cluster_status
Cluster condition is eligible to execute pfc_switch_cluster.
```

```
Date Time node IP address status
2012-11-14 07:32:19 server3 192.168.240.1 ACT
2012-11-14 07:32:19 server4 192.168.240.2 SBY
```

Tip

In execution example above, the place in bold is checkpoint, and the IP address is an example.

Tip

About execution Conditions of the pfc_dual_cluster Command（pfc_dual_cluster --switchover), refer to *7.3.1 Options and Execution Conditions of the pfc_dual_cluster Command* in *Configuration Guide*

2. When execute switchover command without specifying a backup file, confirm that the backup file exists in the appointed location in active and standby PFC servers of reserve cluster.

   Run the following command to confirm.

```
ls /var/opt/nec/pfc/archive/mgmt/back_20121101110052_V5.0.0.0build1.tar.gz
/var/opt/nec/pfc/archive/mgmt/back_20121101110052_V5.0.0.0build1.tar.gz
```

Tip

In execution example above, the place in bold is checkpoint, and the file-name is an example.

2.7 Trouble with Backup/Restore

2.7.1 A restore command was executed without specifying the -l option

Execute the `pfc_show_cluster_status` command on the standard shell. If `Mirror disk status is XXX.` is not displayed, a mirror disk is not used and thus no action is required.

```
# pfc_show_cluster_status
        :
Mirror disk status is Normal.
        :
```

When using a mirror disk, recovery is possible before switching the PFC server on which the restore command was executed to the active node. Execute the command below to delete the temporary directory for mirror disk restoration (`/var/opt/nec/pfc/Agent/tmp/mgmt/mirror`).

```
# rm -rf /var/opt/nec/pfc/Agent/tmp/mgmt/mirror
```

If the temporary directory for restoration does not exist, the PFC has already been switched to the active node, so mirror disk restoration is complete and the directory has been deleted.

Chapter 3. Procedure to Gather Information

This chapter mainly explains the procedure for gathering information about failures.

3.1 Gathering Information about Failures

Using the `show tech-support` command, it is possible to gather all information when failures occur. Using the `dump` command, it is possible to gather the memory dump when failures occur. Regarding gathering information when failures occur, confirm with the support staff first which failure information is needed

3.1.1 Using the show tech-support command to gather information about failures

When requested to use the `show tech-support` command, run the following from the PFC Shell, and gather the information by using the command line below.

```
# show tech-support > /home/pfcadmin/<File name>
```

In the file name of the redirect destination, make sure to specify the path name of the home directory of the logged in user.

If any other directory or related path name is specified, the command will fail.

Important

Executing the `show tech-support` command puts a load on the secure channel and may affect communication processing. So execute this command only when instructed to by the maintenance and service company.

Tip

During execution of the `show tech-support` command, the result display may take time depending on the environment. To cancel the execution of the `show tech-support` command, press the **Ctrl**+**C** keys to forcibly stop the processing.

3.1.2 Using the dump command to gather information about failures

When requested to use the `dump` command, gather the information by executing the `pfc_dump` command in the standard shell.

```
# pfc_dump dump --all
```

The dump obtained by using the `pfc_dump` command will be created with the file name below.

`/var/opt/nec/pfc/archive/mgmt/dump/dump_<date and time created>_<Version>.tar.gz`

Chapter 4. Procedure for Replacement

This chapter describes how to recover the PFC server when hardware or software is replaced.

4.1 Recovery Procedure upon Hardware/Software Replacement

This chapter describes the PFC recovery procedure when the hardware and software of PFC1 (active node) are replaced in an active/standby cluster configuration that consists of PFC1 and PFC2.

Tip

When replacing the hardware and software of both nodes, perform the procedure for both PFC1 and PFC2. It is recommended to start from the standby node.

4.1.1 Preparation before replacing hardware and software

This section describes the preparation to be performed before hardware and software replacement. Follow the procedure shown below.

1. Check that the cluster status of PFC1 is active.

```
# pfc_show_cluster_status
Cluster condition is eligible to execute pfc_switch_cluster.

Date       Time      node  IP address        status
2014-08-01 14:26:12  PFC1  192.168.251.251   ACT
2014-08-01 14:27:06  PFC2  192.168.251.252   SBY
```

2. Back up the PFC server software data on PFC1.

```
# pfc_backup backup
..
Backup has done
```

3. Check the backup file on PFC1.

```
# pfc_backup list

Date       Time     Version         Size    File
2014-08-01 14:36:11 V6.0.0.0buildXX 1133343 back_20140801143611_V6.0.0.0buildXX.tar.gz
   :             :
```

4. Connect the PC to PFC1 via ftp, and then log in as an Administrator.

```
# ftp <IP address of PFC1>
   :             :
Name (<IP address of PFC1>:root): pfcadmin   Enter a user name.
331 Please specify the password.
Password:                                    Enter a password.
230 Login successful.
   :             :
```

5. Download the backup file.

   (The backup file is created under `/var/opt/nec/pfc/archive/mgmt/backup`.)

```
ftp> cd /var/opt/nec/pfc/archive/mgmt/backup
                          Move to the directory to store the backup file.
250 Directory successfully changed.
ftp> ls                    Display the files in the directory.
   :             :
-rw-r-----    1 root     pfcadmin  1133343 Aug 01 14:36 back_20140801143611_V6.0.0.0buil
dXX.tar.gz
   :             :
ftp> bin                  Set the binary transfer mode.
200 Switching to Binary mode.
ftp> get back_20140801143611_V6.0.0.0buildXX.tar.gz
                          Download the backup file.
local: back_20140801143611_V6.0.0.0buildXX.tar.gz remote: back_20140801143611_V6.0.0.0bu
ildXX.tar.gz
   :             :
226 Transfer complete.
   :             :
ftp> bye                  Exit ftp.
```

4.1.2 Replacing hardware/software

After completing the procedures according to "4.1.1 Preparation before replacing hardware and software (page 35)", replace the hardware/software, following the procedure shown below.

1. Switch PFC1 to the standby node. (Skip this step if PFC1 is already a standby node.)

```
# pfc_switch_cluster
Cluster switchover was launched.
```

2. Check that PFC1 is a standby node.

```
# pfc_show_cluster_status
Cluster condition is not eligible to execute pfc_switch_cluster
by the following reason.
    * This node is not ACT.
      pfc_switch_cluster is executable only at ACT node.

Date       Time      node  IP address        status
2014-08-01 14:26:12  PFC1  192.168.251.251   SBY
2014-08-01 14:27:06  PFC2  192.168.251.252   ACT
```

3. Shut down PFC1.

```
# shutdown -h now
   :             :
The system is going down for halt NOW!
```

4. Replace the PFC1 hardware if required.
5. Perform PFC1 installation of OS according to *2.2 Installing PFC (When OS is necessary to be installed)* in the *Installation Guide*.
6. Perform PFC1 network settings according to *2.4.1 Network Interface Settings for PFC* in the *Installation Guide*.
7. Perform PFC1 network settings according to *2.4.2 Network Settings* in the *Installation Guide*.
8. Connect the PC to PFC1 via ftp, and then log in as an Administrator.

```
# ftp <IP address of PFC1>
   :             :
Name (<IP address of PFC1>:root): pfcadmin    Enter a user name.
331 Please specify the password.
Password:                                     Enter a password.
230 Login successful.
   :             :
```

9. Upload the backup file that was downloaded to the PC.

```
ftp> cd /var/opt/nec/pfc/archive/mgmt/backup
                          Move to the directory to store backup files.
250 Directory successfully changed.
ftp> bin                 Set the binary transfer mode.
200 Switching to Binary mode.
ftp> put back_20140801143611_V6.0.0.0buildXX.tar.gz
                       Upload the backup file.
local: back_20140801143611_V6.0.0.0buildXX.tar.gz remote: back_20140801143611_V6.0.0.0bu
ildXX.tar.gz
   :             :
226 Transfer complete.
   :             :
ftp> bye               Exit ftp.
```

10. Restore the PFC server software data to PFC1.

```
# pfc_backup restore back_20140801143611_V6.0.0.0buildXX.tar.gz -l -s
Are you sure you want to restore the data? (y/N) y    Enter y.
...
Restore has done. Please reboot your system.
```

Important

- Do not reboot the system at this step even though "Please reboot your system." is displayed.
- The user settings are not restored. Perform settings as required by referring to *5.1 User Management* in the *Configuration Guide*.

11. Recover the mirror disk as required.

Remember

Skip this step if any of the following conditions applies:

- A mirror disk is not used.
- The PFC server running on the active node is using the mirror disk.

```
# pfc_backup restore back_20140801143611_V6.0.0.0buildXX.tar.gz
Are you sure you want to restore the data? (y/N) y     Enter y.
...
Restore has done. Please reboot your system.
```

Important

- Do not reboot the system at this step even though `Please reboot your system.` is displayed.
- After performing this procedure, be sure to switch to the active node after hardware/software replacement is complete.

12. Declare that PFC2 is the synchronization source of the cluster settings.

```
# pfc_setup_redundancy --master resync
Completed the registration.
Please execute "pfc_setup_redundancy --follower" on PFC1.
*** BE CAREFUL ***
   After you execute "pfc_setup_redundancy --follower", data held
   on PFC1 will be overwritten by PFC2's.
```

13. Declare that PFC1 is the synchronization destination of the cluster settings.

```
# pfc_setup_redundancy --follower
Cluster setup preparation was completed.
```

14. Change the PFC1 startup settings.

```
# chkconfig clusterpro on
# chkconfig pfc_csm_prestart on
# chkconfig pfc_csm on
# chkconfig pfc_sdb on
# chkconfig pfc_nomg on
# chkconfig pfc_csm_prestop on
```

15. Reboot PFC1.

```
# reboot
   :             :
The system is going down for reboot NOW!
```

16. After rebooting, check that PFC1 is included to the cluster as a standby node.

```
# pfc_show_cluster_status
Cluster condition is not eligible to execute pfc_switch_cluster
by the following reason.
    * This node is not ACT.
      pfc_switch_cluster is executable only at ACT node.

Date       Time      node  IP address        status
2014-08-01 14:30:12  PFC1  192.168.251.251   SBY
2014-08-01 14:27:06  PFC2  192.168.251.252   ACT
```

PF6800 Ver. 6.0
Troubleshooting Guide

PFC00EK0600-01

July, 2014 1st Edition

NEC Corporation