PF6800 Ver. 6.1
PFTAP User's Guide

PFC00EY0610-01

Copyrights

Information in this manual may not include all information disclosed by NEC Corporation or may use different expressions than information disclosed by other means. Also, this information is subject to revision or removal without prior notice.

Although every effort has been made to ensure accuracy in producing this manual, NEC Corporation does not guarantee the accuracy or applicability of the information contained herein. In addition, NEC Corporation is not liable for any damages that may occur due to the use or non-use of this information by any party. Translation or reproduction of all or part of this document by any means including electronic, mechanical, or recording means is prohibited unless authorized in writing by NEC Corporation.

Trademarks

- The NEC logo is a registered trademark or a trademark of NEC Corporation in Japan and other countries.
- Microsoft and the Microsoft logo are registered trademarks of Microsoft Corporation (USA).
- Windows is a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.
- Linux is a registered trademark or trademark of Linus Torvalds in Japan and other countries.
- Other company names and product names are trademarks or registered trademarks of their respective companies. Trademark symbols such as TM or ® are not indicated in the main text.

Introduction

Thank you for purchasing PF6800 (referred to as PFC). The PF6800 is a path control device used for centralized management of networks, and conforms to OpenFlow 1.0/1.3.

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 guide describes how to use PFTAP.

Throughout this guide, PFC refers to PF6800, and OFS refers to an OpenFlow switch.

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

Text Conventions of Command Syntax

In this manual, the command syntax is described according to the following text conventions.

1. Parameters for which a desired numeric value or characters is specified are in < >.
2. Enter a character string that is not in < > as is.
3. {A | B} means to select A or B.
4. A parameter in [ ] can be omitted.
5. {[A] | [B]} means to select either or both of A and B.
6. A-B means the value range. For example, 1-100 means that a value in the range of 1 to 100 can be specified.

1 through 5 above are called parameters in this manual (4 may be called an option).

The fixed parameter character string entered following the command name in the standard shell command is called a subcommand.

When multiple parameters are described, "Default value when omitted:" in the description of each command means the case where all of the parameters are omitted.

Structure of this Manual

This manual consists of three chapters. The following is a description for each chapter in this manual.

"Chapter 1. Overview (page 1)"

This chapter describes an overview of PFTAP.

"Chapter 2. Preparation (page 8)"

This chapter describes the initial settings required to use PFTAP.

"Chapter 3. Configuration (page 10)"

This chapter describes how to configure PFTAP.

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. Overview

Following describes an overview of PFTAP.

1.1 Overview of PFTAP

PFTAP is a function for filtering the traffic input from network equipment or a network tap to the OpenFlow network and then transmitting that filtered traffic to an external device, such as a network traffic monitor or packet analysis network analyzer. After entering a match condition for the traffic to be pre-transmitted to PFC, you can register a flow entry that satisfies the match condition to OFS.

1.1.1 OpenFlow Network Structure

The following figure shows an example of the PFTAP OpenFlow network structure. Equipment that duplicates traffic, such as a network device or network tap in the external network, is connected to the OFSs at the input of the OpenFlow network. External device, such as a traffic monitor or network analyzer, is connected to the OFSs at the output of the OpenFlow network.

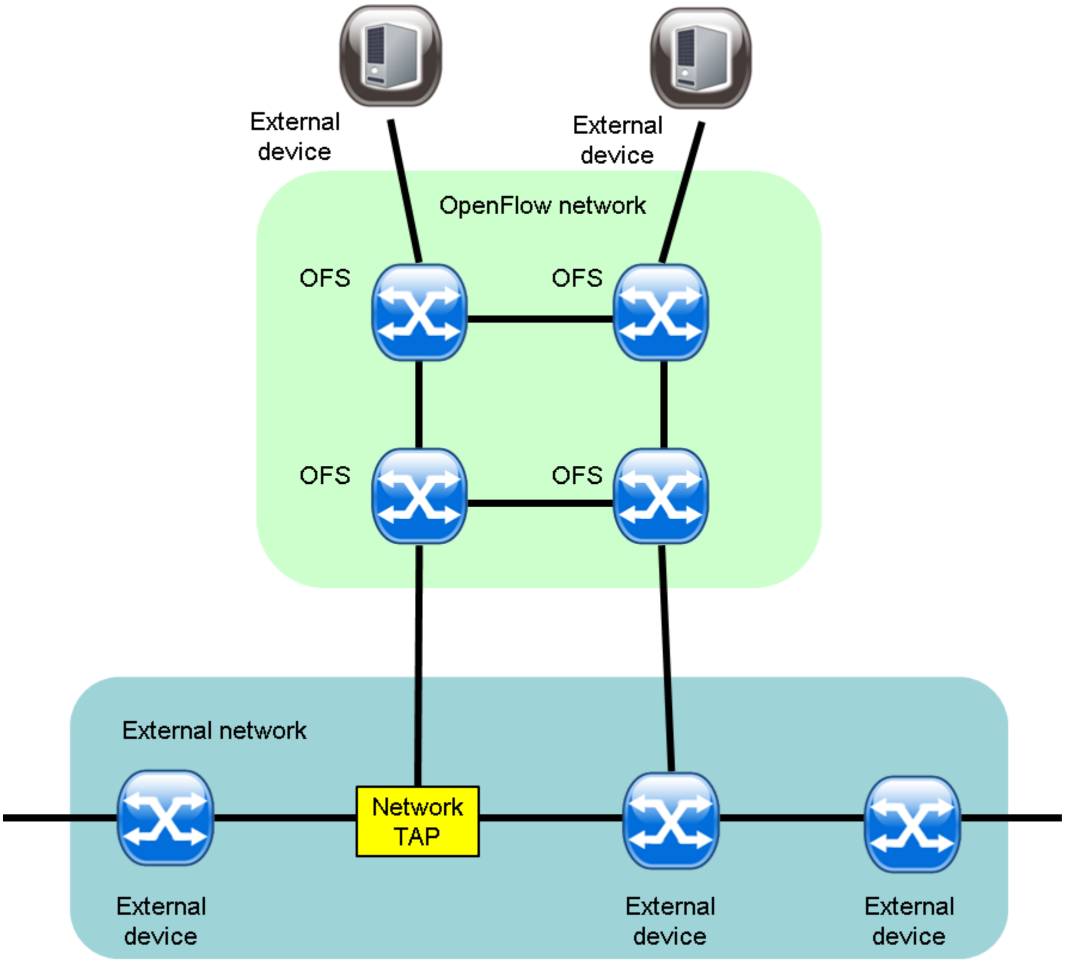

Figure 1-1 OpenFlow Network Structure

Important

Traffic cannot be duplicated within the OpenFlow network. Rather, it is necessary to input traffic that has already been duplicated in an external network to the OpenFlow network.

1.1.2 Virtual Network Structure

The following figure shows an example PFTAP virtual network structure. Using the safe flow filter, PFTAP registers a flow entry that transmits traffic to the OFS. The VTN is configured as follows:

1. Register a VTN.
2. Register a vExternal to the VTN. Use ofs-map to map an OFS port for inputting traffic from the external network and an OFS port for outputting traffic to external devices. The ofs-map command allows you to either specify a VLAN ID value directly or specify all VLANs.
3. Register a flow list and specify a match condition for the traffic you want to transmit. You can use the safe flow filter to specify the match conditions to be applied.
4. Register the safe flow filter with the vExternal interface to which an OFS port for traffic input has been mapped. Specify the flow list registered in Step 3. As its action, specify the redirect action and also specify, as the destination virtual node, the vExternal to which an OFS port for traffic output has been mapped.

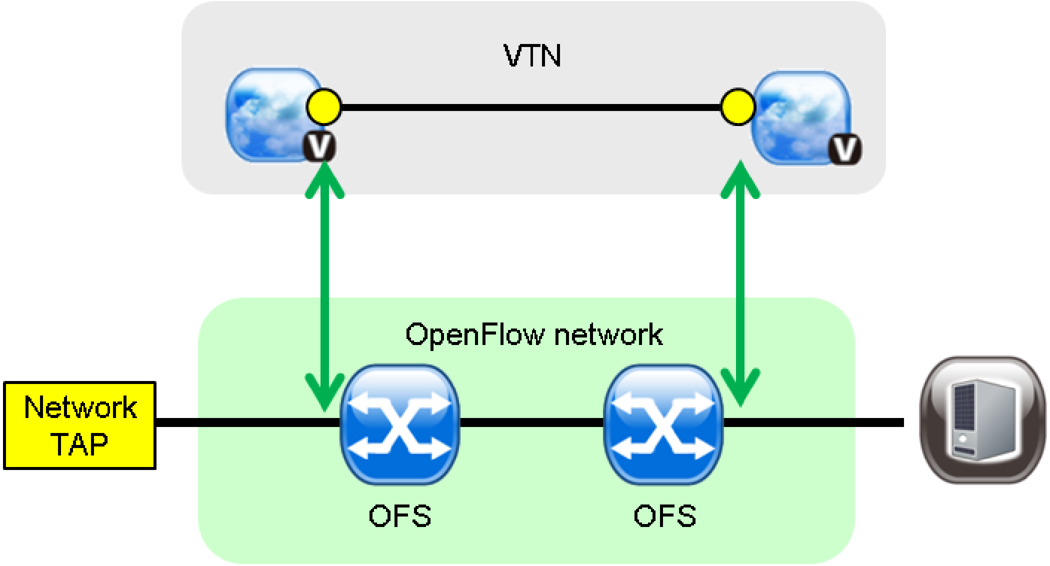

Figure 1-2 Virtual Network Structure

Tip

Specifying VLAN ID-4095 specifies all VLANs including those without VLAN-tag (untagged).

1.1.3 Flow Registration Processing

The following figure shows an example of the PFTAP flow registration processing. The PFC registers a flow entry to transmit packets that satisfy the match condition for the safe flow filter of the PFC to the input OFS. Traffic that does not satisfy the match condition of the safe flow filter is dropped at the input OFS. By receiving traffic from the OFS, the PFC generates a flow to transmit traffic, to the external device, that satisfies the match condition and then registers a flow entry with the OFS.

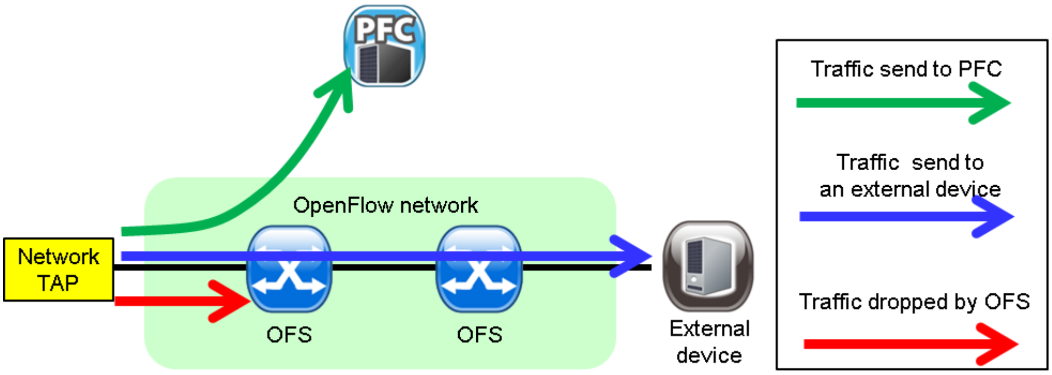

Figure 1-3 Flow Registration Processing

1.2 Match Conditions Supported by PFTAP

The following table lists the commands that correspond to the match conditions supported by PFTAP.

Table 1-1 Match Conditions Supported by PFTAP and Corresponding Commands

Match Condition	Command
Input port	ofs-port option of the ofs-map command in the vexternal config-mode
VLAN ID	vlan-id option of the ofs-map command in the vexternal config-mode
Destination MAC address	mac-destination-address command in the Flow-List-Sequence config-mode
Source MAC address	mac-source-address command in the Flow-List-Sequence config-mode
Destination IPv4 address and prefix length	ip-destination-address command in the Flow-List-Sequence config-mode
Source IPv4 address and prefix length	ip-source-address command in the Flow-List-Sequence config-mode
Destination IPv6 address and prefix length	ipv6 ip-destination-address command in the Flow-List-Sequence config-mode
Source IPv6 address and prefix length	ipv6 ip-source-address command in the Flow-List-Sequence config-mode
IP header protocol	ip-protocol command in the Flow-List-Sequence config-mode
TCP/UDP destination port number	l4-destination-port command in the Flow-List-Sequence config-mode
TCP/UDP source port number	l4-source-port command in the Flow-List-Sequence config-mode

1.3 OFSs Supporting PFTAP

The following table lists the OFS versions and usage supported by PFTAP.

Table 1-2 OFS Usages and Versions That Support PFTAP

OFS Usage	PF52xx	PF54xx	PF5820	PF1000
Edge switch	V5.1 or later	V7.1.11 or later [*1*2]	V7.6 or later [*2]	Not supported
Core switch	V5.1 or later	V7.1.11 or later	V7.6 or later	Not supported

[*1] Transmission of traffic without VLAN-tag (untagged) is not supported

[*2] A flow list that specifies an IPv6 address is not supported

1.4 Supported PFC Functions When Using PFTAP

When using PFTAP, the number of supported PFC functions is limited. The following table lists the relationship between the functions provided by PFC and the OFS usage when using PFTAP. The table lists the OFS types that each function can use.

Table 1-3 Functions Supported by PFC and OFS Usages When Using PFTAP

Provided Function	Edge Switch	Core Switch	Remark
L2 switching	N	N	The vbridge command in vtn config-mode cannot be registered with candidate-configuration.
IPv4 transmission	N	N	The vrouter command in vtn config-mode cannot be registered with candidate-configuration.
IPv6 transmission	N	N	The vrouter command in vtn config-mode cannot be registered with candidate-configuration.
Flow filtering function (L2, IPv4 match conditions)	PF52xx PF54xx PF5820	Y	The flow filtering function can be used only with the flow-filter-safe command in interface config-mode. The flow-filter command in vtn or interface config-mode cannot be registered with candidate-configuration.
Flow filtering function (IPv6 match condition specified)	PF52xx	Y	The flow filtering function can be used only with the flow-filter-safe command in interface config-mode. The flow-filter command in vtn or interface config-mode cannot be registered with candidate-configuration.
Policing function	PF52xx	Y	
Flooding packet policing	N	N	
DSCP marking	N	N	
Transmission priority	N	N	
IGMP/MLD Proxy function	N	N	
Extended VLAN mode	N	N	The vlan-connect enable command in real-network config-mode cannot be registered with candidate-configuration.
Port group function	PF52xx	PF52xx	
Administrative status initialization function of the OFS port	Y	Y	
Link down relay function	Y	Y	

Provided Function	Edge Switch	Core Switch	Remark
VLAN automatic setting function	N	N	
Bandwidth monitoring function	Y	Y	
Flow entry count monitoring function	Y	Y	
sFlow monitoring function (by the GUI)	N	N	
MCLAG	N	N	The trunk-port and trunk-port-group commands in real-network config-mode cannot be registered with candidate-configuration.
Logical link failure high-speed detection function	PF52xx	PF52xx	
MAC mapping	N	N	
OpenFlow1.3 function	PF52xx PF54xx	PF52xx PF54xx	
GUI	N	N	
Web GUI	Y	Y	
Switch configuration	N	N	
VLAN mapping	N	N	
OFS domain function	Y	Y	
OFS sub-domain function	N	N	The ofs-subdomain command in ofs-domain or ofs-default-domain config-mode cannot be registered with candidate-configuration.
Path policy	Y	Y	

Y: Supported regardless of switch type.

N: Not supported

1.5 Cautions Related to Use of PFTAP

Following describes cautions when using PFTAP.

1.5.1 Condition That Does Not Allow the Use of PFTAP

PFTAP cannot be used with PFC that has been upgraded from a version earlier than V6.0.

1.5.2 Command Differences When PFTAP Is Enabled

When PFTAP is enabled, the following commands will differ.

- When specifying 4095 with the vlan-id option of the ofs-map command in vexternal config-mode, you can map all the VLANs including those without VLAN-tag (untagged). You cannot map the port with 4095 specified by the vlan-id option of the ofs-map command in vexternal config-mode to another vExternal using another VLAN ID.

- You can specify between 1 and 16 with the priority command in the flow-filter-safe config-mode.

1.5.3 PFC Settings That Do Not Register Flows

If the following settings are configured on the PFC, any flows that transmit traffic are not registered. Do not configure the following settings on the PFC.

- The pass option of the action command in entry-id config-mode is specified. To register a flow that transmits traffic, specify the redirect option. To register a flow that drops traffic, drop option can be specified.
- The modify-mac-destination or modify-mac-source option of the redirect-destination command in entry-id config-mode is specified.
- The following VLAN IDs are not matched. Specify the same value for the following VLAN IDs or use 4095, which indicates all VLAN IDs.
    - VLAN ID mapped to vexternal to which the safe flow filter is registered
    - VLAN ID mapped to vexternal specified with the vnode option of the redirect-destination command in the entry-id config-mode

1.5.4 Traffic That Does Not Register Flows

Flows are not registered to the following traffic. Do not input the following traffic to the OpenFlow network.

- Traffic with VLAN ID 4094. VLAN ID 4094 is reserved by the PF system.
- Traffic with destination MAC address 00:00:00:00:00:00. Destination MAC address 00:00:00:00:00:00 is reserved by the PF system.

1.5.5 Flow Statistics of PF5459

PF5459 does not support the number of bytes in flow statistics. If following commands are executed with the detail option, the number of bytes or octets in statistics is 0.

- show data-flow(vtn mode)
- show vtn-station
- show path-map
- show flow-filter-safe

1.5.6 Settings for Enabling PFTAP in Upgrading the PFC Version

PFTAP is disabled on the PFC server which is performed PFC upgrade installation.

If you upgrade or downgrade the version on PFC when PFTAP is enabled, run the follow command after perform PFC upgrade installation. Then restart the PFC server.

```
[root@pfcserver1 ~]# pfc_tap --enable
PFTAP is enabled.
Please reboot system to complete enabling PFTAP.
```

1.5.7 Backing Up Settings for Enabling/Disabling PFTAP

The settings for enabling/disabling PFTAP are backed up or restored by the backup commands. For detail, refer to *Backing Up Data* in the *Configuration Guide*.

Chapter 2. Preparation

Following describes the initial settings required to use PFTAP.

2.1 Settings for Enabling/Disabling PFTAP

To use PFTAP, configure the settings to enable PFTAP when the cluster is stopped. To stop using PFTAP, configure the settings to disable PFTAP when the cluster is stopped.

The settings for enabling/disabling PFTAP are configured in the following order:

1. Stop the cluster function.
2. Run the pfc_tap command.
3. Restarting the PFC server.

Important

- To configure the settings for enabling/disabling PFTAP, log in to the PFC server as a root user.
- The settings for enabling/disabling PFTAP must be configured on both the active and standby PFC servers configuring the cluster.
- There is no running-configuration compatibility between when PFTAP is enabled and disabled. When using PFC before enabling PFTAP, startup-configuration must be deleted before configuring the settings for enabling PFTAP. Before performing the steps described here, delete startup-configuration by executing the clear startup-configuration command. Before configuring the settings for disabling PFTAP, again delete startup-configuration.

2.1.1 Stopping the Cluster Function

Before configuring the PFTAP initial settings, stop the cluster function. This must be done on both the active and standby PFC servers.

1. Stop the cluster function. Run the following command.

```
[root@pfcserver1 ~]# pfc_stop_cluster
Cluster will be stopped.
```

After about a minute, the message "Cluster will be stopped." will be displayed and the cluster will be stopped normally.

2. Check the cluster status. Run the following command.

```
[root@pfcserver1 ~]# pfc_show_cluster_status
Cluster not started.
```

The cluster stops and the message "Cluster not started." is displayed.

2.1.2 Executing the pfc_tap Command

Run the pfc_tap command to enable or disable PFTAP. This must be done on both the active and standby PFC servers.

Run the following command.

- [To enable PFTAP]

```
[root@pfcserver1 ~]# pfc_tap --enable
PFTAP is enabled.
Please reboot system to complete enabling PFTAP.
```

- [To disable PFTAP]

```
[root@pfcserver1 ~]# pfc_tap --disable
PFTAP is disabled.
Please reboot system to complete disabling PFTAP.
```

2.1.3 Restarting the PFC Server

Run the reboot command to restart the PFC server. This must be done on both the active and standby PFC servers.

```
[root@pfcserver1 ~]# reboot
Broadcast message from root (pts/0) (Tue Jan 31 12:30:05 2012):
The system is going down for reboot NOW!
```

After the PFC server restarted, confirm that PFTAP has been enabled or disabled.

Run the following command.

- [To enable PFTAP]

```
[root@pfcserver1 ~]# pfc_tap --status
PFTAP is enabled.
```

- [To disable PFTAP]

```
[root@pfcserver1 ~]# pfc_tap --status
PFTAP is disabled.
```

Chapter 3. Configuration

Following describes how to configure PFTAP.

3.1 Recommended PFTAP Settings

3.1.1 Overview

Following describes the recommended settings for using PFTAP.

3.1.2 Configuration Diagram and Conditions

[Configuration Diagram]

The following figure shows an example PFTAP OpenFlow network configuration.

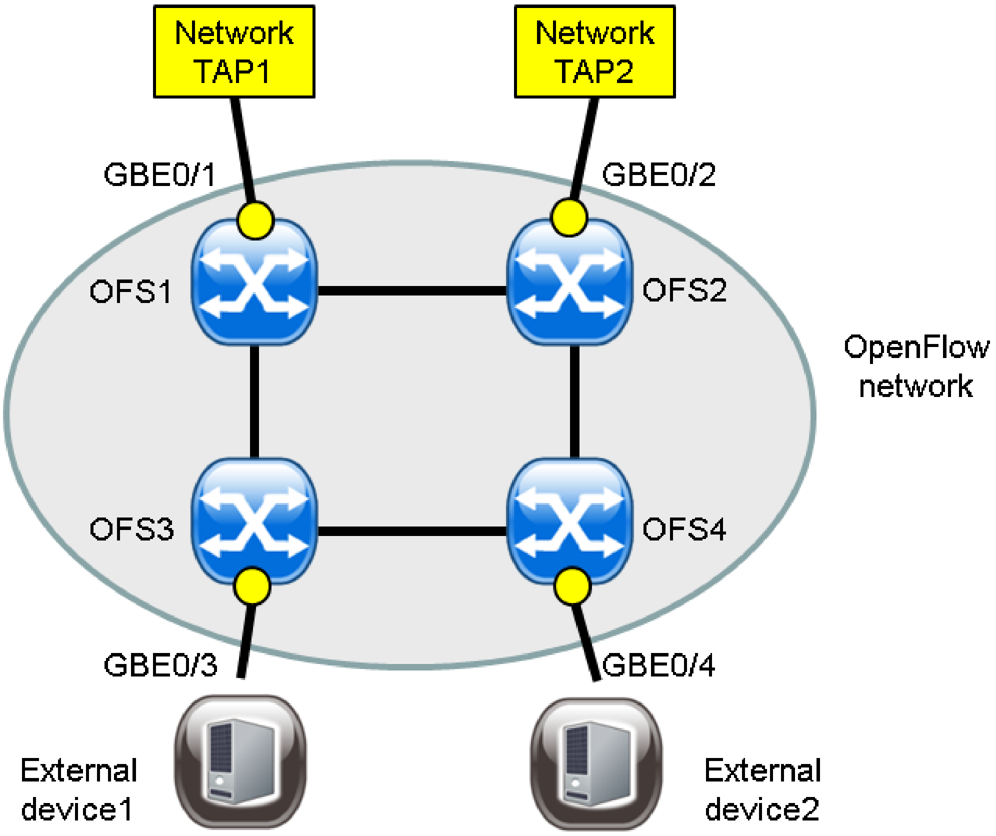

Figure 3-1 Example Configuration of OpenFlow Network

[Conditions]

- The datapath ids of the OFSs are as listed in the following table.

Table 3-1 OFS Setting Information

OFS Name	datapath id
OFS1	0001-0001-0001-0001

OFS Name	datapath id
OFS2	0002-0002-0002-0002
OFS3	0003-0003-0003-0003
OFS4	0004-0004-0004-0004

- If an OFS that supports OpenFlow1.3, such as PF54xx, exists in the OpenFlow network, enable the OpenFlow1.3 function.
- When using an OFS with only a small number of flow entries that can be registered, such as PF5820 or PF5459, specify a short period of time for aging in the VTN station. Because as many flow entries as the number of VTN stations are registered for the edge switch, the time required before deleting any unnecessary flow entries is shortened.
- Set an OFS port connected to the external network or device as the external port. When no external port is set, PLDP packets are transmitted from the PFC to the external network or devices.
- If PF52xx exists in the OpenFlow network, enable the port group function to accelerate the rerouting process.

3.1.3 Sample Setting and Description

The following describes a configuration example.

[Sample Command List]

```
network-default {
  openflow-version 1.3                                                          (1)
  vtn-station aging-time 60                                                     (2)
}
real-network {
  ofs 1 {                                                                       (3)
    datapath 0001-0001-0001-0001                                                (4)
    port "GBE0/1" {                                                             (5)
      external-port                                                             (6)
    }
  }
  ofs 2 {                                                                       (7}
    datapath 0002-0002-0002-0002                                                (8)
    port "GBE0/2" {                                                             (9)
      external-port                                                             (10)
    }
  }
  ofs 3 {                                                                       (11)
    datapath 0003-0003-0003-0003                                                (12)
    port "GBE0/3" {                                                             (13)
      external-port                                                             (14)
    }
  }
  ofs 4 {                                                                       (15)
    datapath 0004-0004-0004-0004                                                (16)
    port "GBE0/4" {                                                             (17)
      external-port                                                             (18)
    }
  }
  port-group enable                                                             (19)
}
```

[Description]

Table 3-2 Description of Commands

Number	Description
(1)	Enable OpenFlow 1.3.

Number	Description
(2)	Set the aging time to 60 seconds in the VTN station.
(3) and (4)	To the OFS with datapath id 0001-0001-0001-0001, assign the ID as 1.
(5) and (6)	For ofs 1, create the port "GBE0/1" and set it as the external port.
(7) and (8)	To the OFS with datapath id 0002-0002-0002-0002, assign the ID as 2.
(9) and (10)	For ofs 2, create the port "GBE0/2" and set it as the external port.
(11) and (12)	To the OFS with datapath id 0003-0003-0003-0003, assign the ID as 3 .
(13) and (14)	For ofs 3, create the port "GBE0/3" and set it as the external port.
(15) and (16)	To the OFS with datapath id 0004-0004-0004-0004, assign the ID as 4.
(17) and (18)	For ofs 4, create the port "GBE0/4" and set it as the external port.
(19)	Enable the port group function.

3.2 Filtering Traffic by Specifying an OFS Port or Both a Port and VLAN

3.2.1 Overview

By specifying an OFS port as a match condition for filtering traffic, all received traffic is transmitted to the external devices. Or, by specifying both an OFS port and a VLAN ID value as a match condition, only specific VLAN traffic is transmitted to the external devices.

3.2.2 Configuration Diagram and Conditions

[Configuration Diagram]

The following figure shows an example configuration for filtering traffic with an OFS port or a port and VLAN specified. The network taps are connected to OFS1 GBE0/1 and OFS2 GBE0/2, and traffic is input from the external network to the OpenFlow network. From network tap 1, VLAN 10 traffic is input. From network tap 2, VLAN 100 and 200 traffic is input. External devices are connected to OFS3 GBE0/3 and OFS4 GBE0/4, and filtered traffic is then transmitted to them.

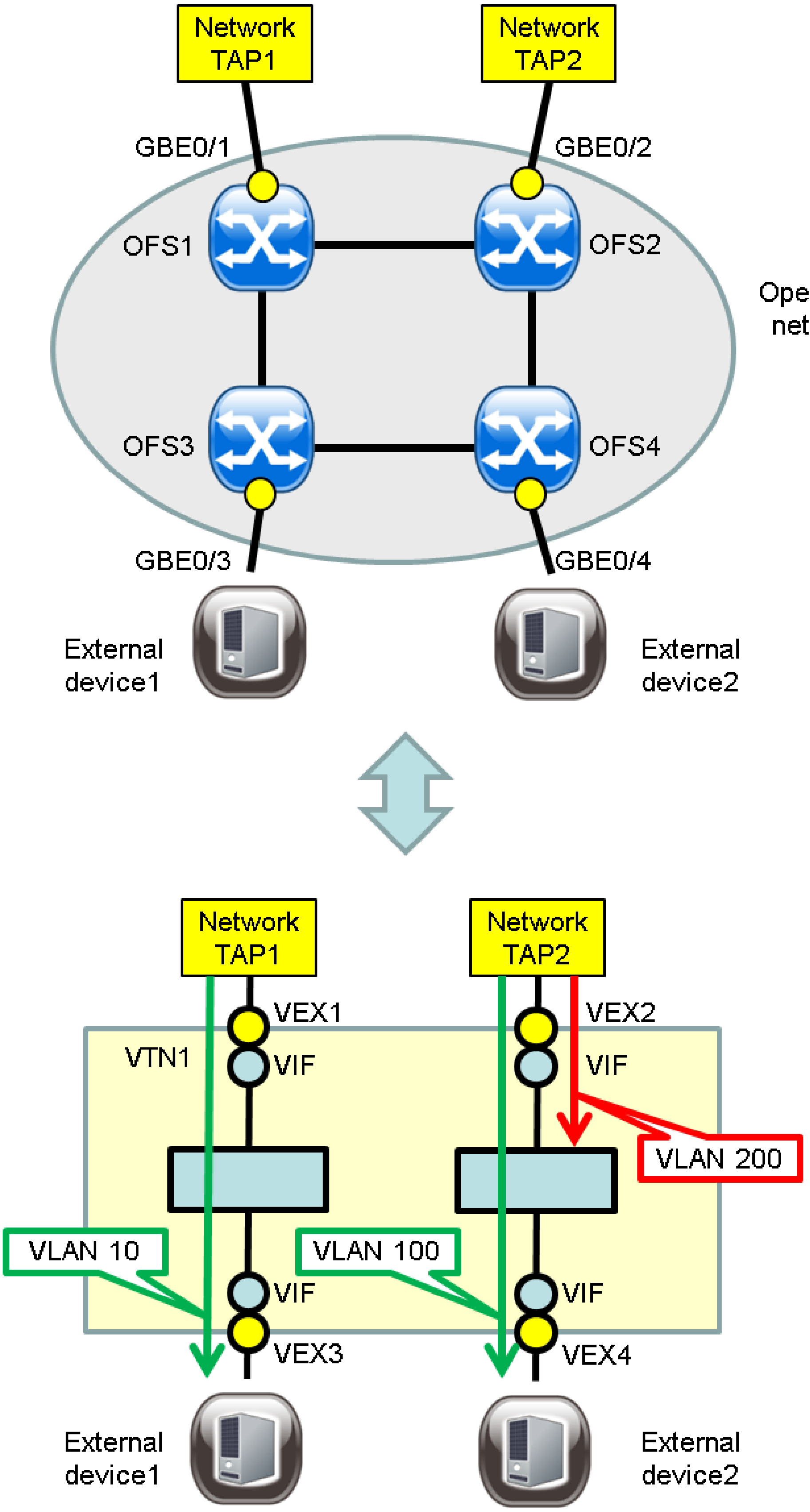

Figure 3-2 Example Configuration for Filtering Traffic by Specifying an OFS Port or Both a Port and VLAN

[Conditions]

- The relationship between the OFS ports and vExternals is as shown in the above figure.
- The datapath ids of the OFSs are as listed in the following table.

Table 3-3 OFS Setting Information

OFS Name	datapath id
OFS1	0001-0001-0001-0001
OFS2	0002-0002-0002-0002
OFS3	0003-0003-0003-0003
OFS4	0004-0004-0004-0004

- All traffic input from OFS1 GBE0/1 is transmitted to external device 1 connected to OFS3 GBE0/3.
- VLAN 100 traffic input from OFS2 GBE0/2 is transmitted to external device 2 connected to OFS4 GBE0/4.
- All but VLAN 100 traffic input from OFS2 GBE0/2 is dropped at OFS2.

3.2.3 Sample Setting and Description

The following describes an example of applying the safe flow filter to a virtual interface.

[Sample Command List]

```
vtn VTN1 {                                                                     (1)
  vexternal VEX1 {                                                             (2)
    ofs-map ofs-datapath-id 0001-0001-0001-0001 ofs-port GBE0/1 vlan-id 4095   (3)
    interface VIF {                                                            (4)
      flow-filter-safe {                                                       (5)
        priority 1 restrict allany {                                           (6)
          entry-id 1 {                                                         (7)
            match allany                                                       (8)
            action redirect                                                    (9)
            redirect-destination vnode VEX3 interface VIF                      (10)
          }
        }
      }
    }
  }
  vexternal VEX2 {                                                             (11)
    ofs-map ofs-datapath-id 0002-0002-0002-0002 ofs-port GBE0/2 vlan-id 100    (12)
    interface VIF {                                                            (13)
      flow-filter-safe {                                                       (14)
        priority 1 restrict allany {                                           (15)
          entry-id 1 {                                                         (16)
            match allany                                                       (17)
            action redirect                                                    (18)
            redirect-destination vnode VEX4 interface VIF                      (19)
          }
        }
      }
    }
  }
  vexternal VEX3 {                                                             (20)
    ofs-map ofs-datapath-id 0003-0003-0003-0003 ofs-port GBE0/3 vlan-id 4095   (21)
    interface VIF                                                              (22)
  }
  vexternal VEX4 {                                                             (23)
    ofs-map ofs-datapath-id 0004-0004-0004-0004 ofs-port GBE0/4 vlan-id 100    (24)
    interface VIF                                                              (25)
  }
}
```

[Description]

Table 3-4 Description of Commands

Number	Description
(1)	Create a VTN with the name VTN1.
(2)	Create a vExternal with the name VEX1.
(3)	Map an OFS port to VEX1. Specify VLAN ID=4095, which represents VLAN ANY.
(4) to (5)	Create a virtual interface VIF for VEX1. Apply the safe flow filter to VIF.
(6)	For priority 1, specify the supported match conditions for allany.
(7) to (10)	For entry-id 1, define allany that transmits all traffic as a match condition and set its action to redirect. Specify VIF in VEX3 for a vExternal virtual interface to redirect.
(11)	Create a vExternal with the name VEX2.
(12)	Map an OFS port to VEX2. Specify VLAN ID=100.
(13) to (14)	Create a virtual interface VIF for VEX2. Apply the safe flow filter to VIF.
(15)	For priority 1, specify the supported match conditions for allany.
(16) to (19)	For entry-id 1, define allany that transmits all traffic as a match condition and set its action to redirect. Specify VIF in VEX4 for a vExternal virtual interface to redirect.
(20)	Create a vExternal with the name VEX3.
(21)	Map an OFS port to VEX3. Specify VLAN ID=4095, which represents VLAN ANY.
(22)	Create a virtual interface VIF for VEX3.
(23)	Create a vExternal with the name VEX4.
(24)	Map an OFS port to VEX4. Specify VLAN ID=100.
(25)	Create a virtual interface VIF for VEX4.

[Example of Overall Configuration]

```
network-default {
  openflow-version 1.3
  vtn-station aging-time 60
}
real-network {
  ofs 1 {
    datapath 0001-0001-0001-0001
    port "GBE0/1" {
      external-port
    }
  }
  ofs 2 {
    datapath 0002-0002-0002-0002
    port "GBE0/2" {
      external-port
    }
  }
  ofs 3 {
    datapath 0003-0003-0003-0003
    port "GBE0/3" {
      external-port
    }
  }
  ofs 4 {
    datapath 0004-0004-0004-0004
    port "GBE0/4" {
      external-port
    }
  }
  port-group enable
}
vtn VTN1 {
  vexternal VEX1 {
    ofs-map ofs-datapath-id 0001-0001-0001-0001 ofs-port GBE0/1 vlan-id 4095
    interface VIF {
      flow-filter-safe {
        priority 1 restrict allany {
          entry-id 1 {
            match allany
            action redirect
            redirect-destination vnode VEX3 interface VIF
          }
        }
      }
    }
  }
  vexternal VEX2 {
    ofs-map ofs-datapath-id 0002-0002-0002-0002 ofs-port GBE0/2 vlan-id 100
    interface VIF {
      flow-filter-safe {
        priority 1 restrict allany {
          entry-id 1 {
            match allany
            action redirect
            redirect-destination vnode VEX4 interface VIF
          }
        }
      }
    }
  }
  vexternal VEX3 {
    ofs-map ofs-datapath-id 0003-0003-0003-0003 ofs-port GBE0/3 vlan-id 4095
    interface VIF
  }
  vexternal VEX4 {
    ofs-map ofs-datapath-id 0004-0004-0004-0004 ofs-port GBE0/4 vlan-id 100
    interface VIF
  }
}
```

3.3 Filtering Traffic by Specifying an IPv4 Address

3.3.1 Overview

By specifying the destination IPv4 address as a match condition for filtering traffic, traffic is transmitted to different external devices for each destination IPv4 address. In addition, traffic on a specified TCP destination port is transmitted to other external devices.

3.3.2 Configuration Diagram and Conditions

[Configuration Diagram]

The following figure shows an example configuration for filtering traffic by specifying an IPv4 address. The network tap is connected to OFS1 GBE0/1, and traffic is input from the external network to the OpenFlow network. External devices are connected to OFS2 GBE0/2, OFS3 GBE0/3, and OFS4 GBE0/4, and filtered traffic is transmitted to them.

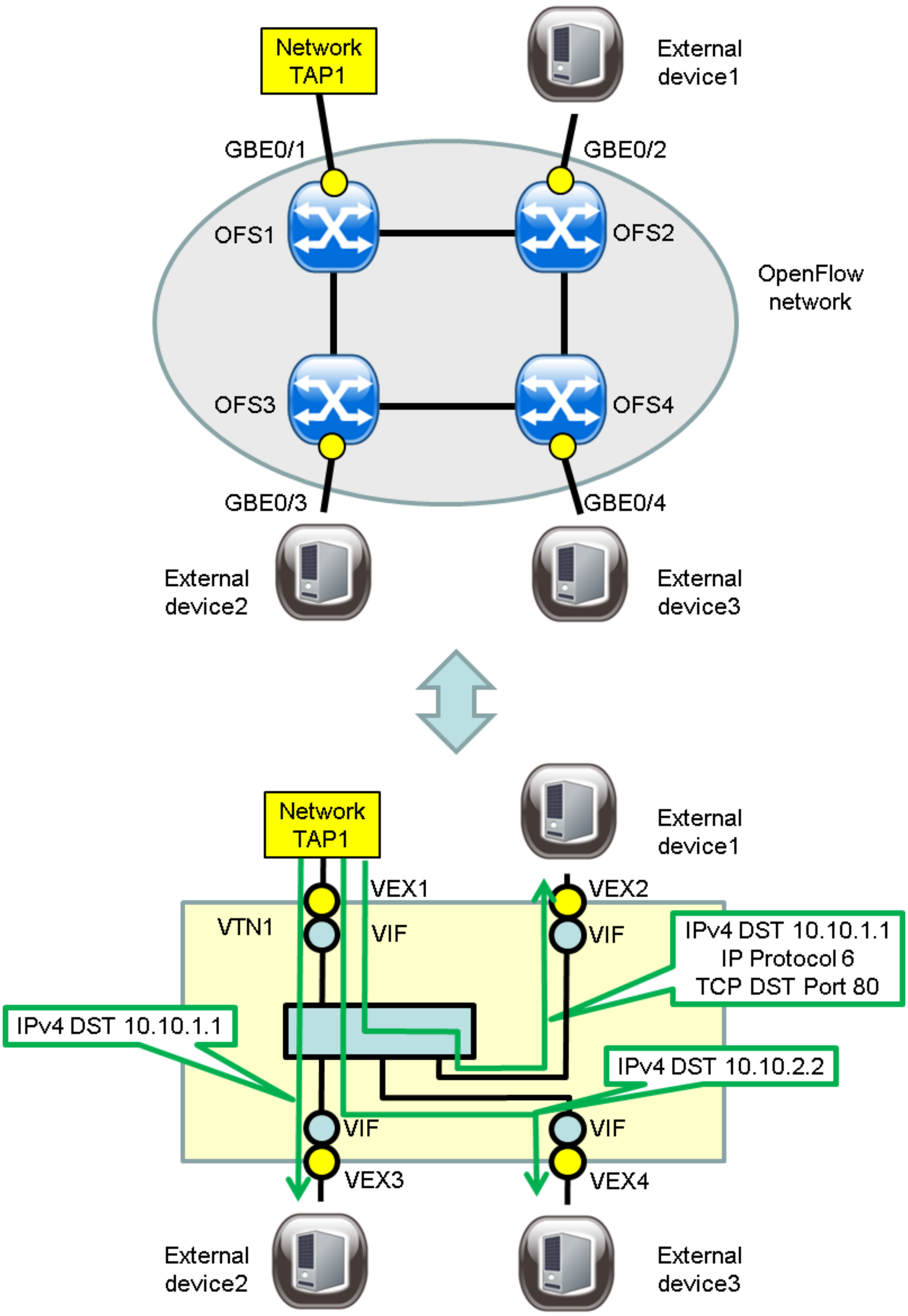

Figure 3-3 Example Configuration for Filtering Traffic by Specifying IPv4 Address

[Conditions]

- The relationship between the OFS ports and vExternals is as shown in the above figure.
- The datapath ids of the OFSs are as listed in the following table.

Table 3-5 OFS Setting Information

OFS Name	datapath id
OFS1	0001-0001-0001-0001

OFS Name	datapath id
OFS2	0002-0002-0002-0002
OFS3	0003-0003-0003-0003
OFS4	0004-0004-0004-0004

- Traffic with destination IPv4 address 10.10.1.1 and TCP destination port number 80, input from OFS1 GBE0/1, is transmitted to external device 1 connected to OFS2 GBE0/2.
- Traffic with destination IPv4 address 10.10.1.1 other than that with TCP destination port number 80, input from OFS1 GBE0/1, is transmitted to external device 2 connected to OFS3 GBE0/3.
- Traffic with destination IPv4 address 10.10.2.2, input from OFS1 GBE0/1, is transmitted to external device 3 connected to OFS4 GBE0/4.
- All traffic other than that with destination IPv4 addresses 10.10.1.1 and 10.10.2.2, input from OFS1 GBE0/1, is dropped at OFS1.

3.3.3 Sample Setting and Description

The following describes an example of applying the safe flow filter to a virtual interface.

[Sample Command List]

```
flow-list IPV4_LIST1 restrict dstip ip-proto dstport {                         (1)
  sequence-number 1 {                                                           (2)
    ip-destination-address 10.10.1.1/32                                         (3)
    ip-protocol 6                                                               (4)
    l4-destination-port 80                                                      (5)
  }
}
flow-list IPV4_LIST2 restrict dstip {                                           (6)
  sequence-number 1 {                                                           (7)
    ip-destination-address 10.10.1.1/32                                         (8)
  }
}
flow-list IPV4_LIST3 restrict dstip {                                           (9)
  sequence-number 1 {                                                           (10)
    ip-destination-address 10.10.2.2/32                                         (11)
  }
}
vtn VTN1 {                                                                      (12)
  vexternal VEX1 {                                                              (13)
    ofs-map ofs-datapath-id 0001-0001-0001-0001 ofs-port GBE0/1 vlan-id 4095   (14)
    interface VIF {                                                             (15)
      flow-filter-safe {                                                        (16)
        priority 2 restrict dstip ip-proto dstport {                            (17)
          entry-id 1 {                                                          (18)
            match flow-list IPV4_LIST1                                          (19)
            action redirect                                                     (20)
            redirect-destination vnode VEX2 interface VIF                       (21)
          }
        }
        priority 1 restrict dstip {                                             (22)
          entry-id 1 {                                                          (23)
            match flow-list IPV4_LIST2                                          (24)
            action redirect                                                     (25)
            redirect-destination vnode VEX3 interface VIF                       (26)
          }
          entry-id 2 {                                                          (27)
            match flow-list IPV4_LIST3                                          (28)
            action redirect                                                     (29)
            redirect-destination vnode VEX4 interface VIF                       (30)
          }
        }
      }
    }
  }
  vexternal VEX2 {                                                              (31)
    ofs-map ofs-datapath-id 0002-0002-0002-0002 ofs-port GBE0/2 vlan-id 4095   (32)
    interface VIF                                                               (33)
  }
  vexternal VEX3 {                                                              (34)
    ofs-map ofs-datapath-id 0003-0003-0003-0003 ofs-port GBE0/3 vlan-id 4095   (35)
    interface VIF                                                               (36)
  }
  vexternal VEX4 {                                                              (37)
    ofs-map ofs-datapath-id 0004-0004-0004-0004 ofs-port GBE0/4 vlan-id 4095   (38)
    interface VIF                                                               (39)
  }
}
```

[Description]

Table 3-6   Description of Commands

Number	Description
(1)	Create a flow list with the name IPV4_LIST1. Use the restrict option to set available match conditions to dstip, ip-proto, and dstport.
(2) to (5)	For sequence-number 1, specify a match condition for destination IPv4 address 10.10.1.1/32 and destination port number 80 for protocol number 6 (TCP) TCP. Unspecified fields are considered as ANY (all matches).
(6)	Create a flow list with the name IPV4_LIST2. Use the restrict option to set available match conditions to dstip.
(7) to (8)	For sequence-number 1, specify a match condition for destination IPv4 address 10.10.1.1/32. Unspecified fields are considered as ANY (all matches).
(9)	Create a flow list with the name IPV4_LIST3. Use the restrict option to set available match conditions to dstip.
(10) and (11)	For sequence-number 1, specify a match condition for destination IPv4 address 10.10.2.2/32. Unspecified fields are considered as ANY (all matches).
(12)	Create a VTN with the name VTN1.
(13)	Create a vExternal with the name VEX1.
(14)	Map an OFS port to VEX1. Specify VLAN ID=4095, which represents VLAN ANY.
(15) to (16)	Create a virtual interface VIF for VEX1. Apply the safe flow filter to VIF.
(17)	For priority 2, set the available match conditions to dstip, ip-proto, and dstport.
(18) to (21)	For entry-id 1, define flow list IPV4_LIST1 as a match condition and set its action to redirect. Specify VIF in VEX2 for a vExternal virtual interface to redirect.
(22)	For priority 1, set the available match conditions to dstip.
(23) to (26)	For entry-id 1, define flow list IPV4_LIST2 as a match condition and set its action to redirect. Specify VIF in VEX3 for a vExternal virtual interface to redirect.
(27) to (30)	For entry-id 2, define flow list IPV4_LIST3 as a match condition and set its action to redirect. Specify VIF in VEX4 for a vExternal virtual interface to redirect.
(31)	Create a vExternal with the name VEX2.
(32)	Map an OFS port to VEX2. Specify VLAN ID=4095, which represents VLAN ANY.
(33)	Create a virtual interface VIF for VEX2.
(34)	Create a vExternal with the name VEX3.
(35)	Map an OFS port to VEX3. Specify VLAN ID=4095, which represents VLAN ANY.
(36)	Create a virtual interface VIF for VEX3.

Number	Description
(37)	Create a vExternal with the name VEX4.
(38)	Map an OFS port to VEX4. Specify VLAN ID=4095, which represents VLAN ANY.
(39)	Create a virtual interface VIF for VEX4.

[Example of Overall Configuration]

```
network-default {
  openflow-version 1.3
  vtn-station aging-time 60
}
real-network {
  ofs 1 {
    datapath 0001-0001-0001-0001
    port "GBE0/1" {
      external-port
    }
  }
  ofs 2 {
    datapath 0002-0002-0002-0002
    port "GBE0/2" {
      external-port
    }
  }
  ofs 3 {
    datapath 0003-0003-0003-0003
    port "GBE0/3" {
      external-port
    }
  }
  ofs 4 {
    datapath 0004-0004-0004-0004
    port "GBE0/4" {
      external-port
    }
  }
  port-group enable
}
flow-list IPV4_LIST1 restrict dstip ip-proto dstport {
  sequence-number 1 {
    ip-destination-address 10.10.1.1/32
    ip-protocol 6
    l4-destination-port 80
  }
}
flow-list IPV4_LIST2 restrict dstip {
  sequence-number 1 {
    ip-destination-address 10.10.1.1/32
  }
}
flow-list IPV4_LIST3 restrict dstip {
  sequence-number 1 {
    ip-destination-address 10.10.2.2/32
  }
}
vtn VTN1 {
  vexternal VEX1 {
    ofs-map ofs-datapath-id 0001-0001-0001-0001 ofs-port GBE0/1 vlan-id 4095
    interface VIF {
      flow-filter-safe {
        priority 2 restrict dstip ip-proto dstport {
          entry-id 1 {
            match flow-list IPV4_LIST1
            action redirect
            redirect-destination vnode VEX2 interface VIF
          }
        }
        priority 1 restrict dstip {
          entry-id 1 {
            match flow-list IPV4_LIST2
            action redirect
            redirect-destination vnode VEX3 interface VIF
          }
          entry-id 2 {
            match flow-list IPV4_LIST3
            action redirect
            redirect-destination vnode VEX4 interface VIF
          }
        }
      }
    }
  }
  vexternal VEX2 {
    ofs-map ofs-datapath-id 0002-0002-0002-0002 ofs-port GBE0/2 vlan-id 4095
    interface VIF
  }
  vexternal VEX3 {
    ofs-map ofs-datapath-id 0003-0003-0003-0003 ofs-port GBE0/3 vlan-id 4095
    interface VIF
  }
  vexternal VEX4 {
    ofs-map ofs-datapath-id 0004-0004-0004-0004 ofs-port GBE0/4 vlan-id 4095
    interface VIF
  }
}
```

3.4 Filtering Traffic by Specifying an IPv6 Address

3.4.1 Overview

By specifying the source IPv6 address as a match condition for filtering traffic, ICMPv6 traffic and traffic with a specified destination IPv6 address is transmitted to other external devices.

3.4.2 Configuration Diagram and Conditions

[Configuration Diagram]

The following figure shows an example configuration for filtering traffic by specifying an IPv6 address. The network tap is connected to OFS1 GBE0/1, and traffic is input from the external network to the OpenFlow network. External devices are connected to OFS2 GBE0/2, OFS3 GBE0/3, and OFS4 GBE0/4, and filtered traffic is transmitted to them.

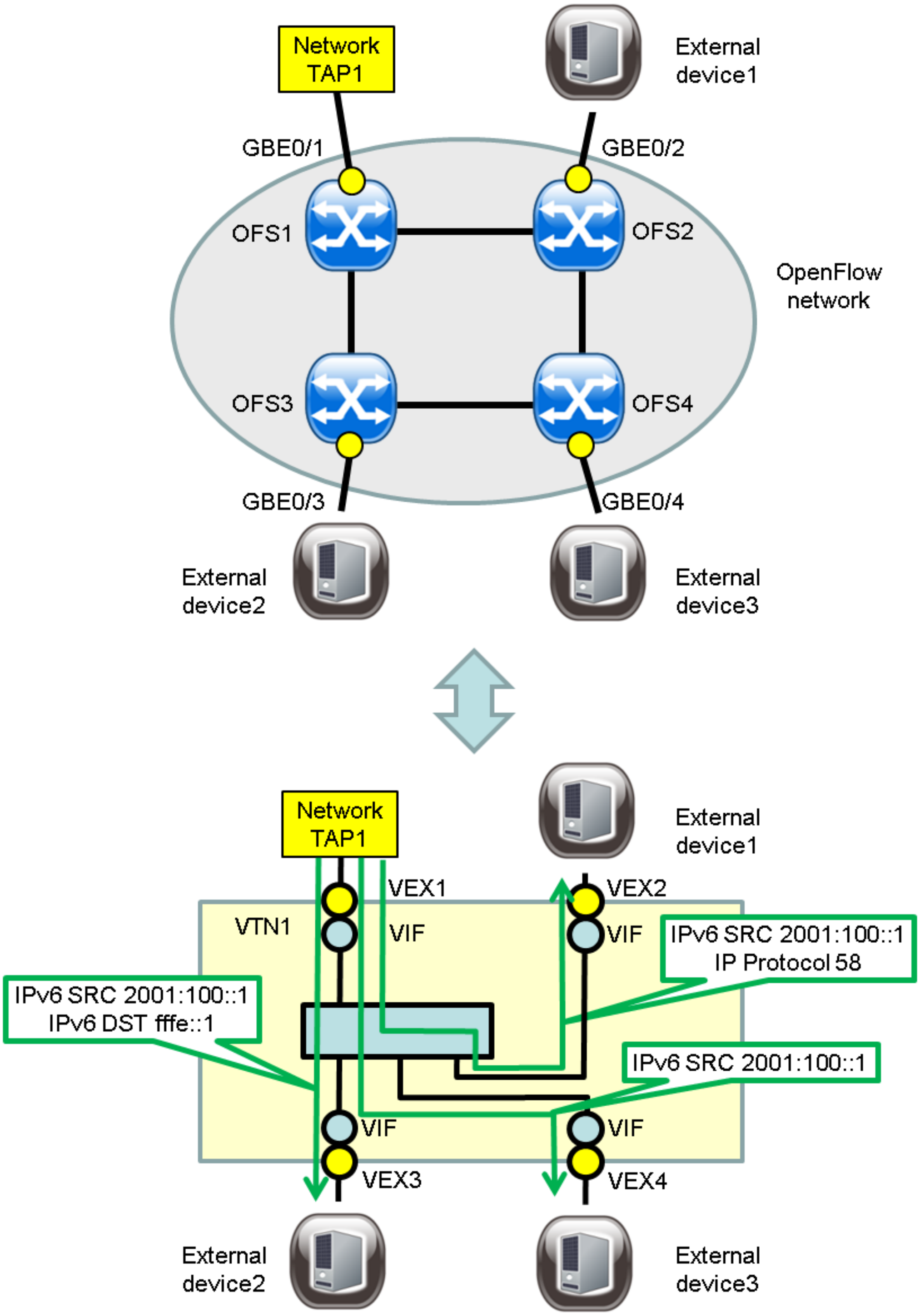

Figure 3-4 Example Configuration for Filtering Traffic by Specifying IPv6 Address

[Conditions]

- The relationship between the OFS ports and vExternals is as shown in the above figure.
- The datapath ids of the OFSs are as listed in the following table.

Table 3-7 OFS Setting Information

OFS Name	datapath id
OFS1	0001-0001-0001-0001

OFS Name	datapath id
OFS2	0002-0002-0002-0002
OFS3	0003-0003-0003-0003
OFS4	0004-0004-0004-0004

- Traffic with source IPv6 address 2001:100::1 and ICMPv6, input from OFS1 GBE0/1, is transmitted to external device 1 connected to OFS2 GBE0/2.
- Traffic with source IPv6 address 2001:100::1 and destination IPv6 address fffe::1 other than that with ICMPv6, input from OFS1 GBE0/1, is transmitted to external device 2 connected to OFS3 GBE0/3.
- Traffic with source IPv6 address 2001:100::1 other than that with destination IPv6 address fffe:: 1 or ICMPv6, input from OFS1 GBE0/1, is transmitted to external device 3 connected to OFS4 GBE0/4.
- All traffic other than that with source IPv6 addresses 2001:100::1, input from OFS1 GBE0/1, is dropped at OFS1.

3.4.3 Sample Setting and Description

The following describes an example of applying the safe flow filter to a virtual interface.

[Sample Command List]

```
flow-list IPV6_LIST1 ipv6 restrict srcip ip-proto {                            (1)
  sequence-number 1 {                                                          (2)
    ip-protocol 58                                                             (3)
    ipv6 ip-source-address 2001:100::1/128                                     (4)
  }
}
flow-list IPV6_LIST2 ipv6 restrict srcip dstip {                               (5)
  sequence-number 1 {                                                          (6)
    ipv6 ip-destination-address fffe::1/128                                    (7)
    ipv6 ip-source-address 2001:100::1/128                                     (8)
  }
}
flow-list IPV6_LIST3 ipv6 restrict srcip {                                     (9)
  sequence-number 1 {                                                          (10)
    ipv6 ip-source-address 2001:100::1/128                                     (11)
  }
}
vtn VTN1 {                                                                     (12)
  vexternal VEX1 {                                                             (13)
    ofs-map ofs-datapath-id 0001-0001-0001-0001 ofs-port GBE0/1 vlan-id 4095   (14)
    interface VIF {                                                            (15)
      flow-filter-safe {                                                       (16)
        priority 3 restrict srcip ip-proto {                                   (17)
          entry-id 1 {                                                         (18)
            match flow-list IPV6_LIST1                                         (19)
            action redirect                                                    (20)
            redirect-destination vnode VEX2 interface VIF                      (21)
          }
        }
        priority 2 restrict srcip dstip {                                      (22)
          entry-id 1 {                                                         (23)
            match flow-list IPV6_LIST2                                         (24)
            action redirect                                                    (25)
            redirect-destination vnode VEX3 interface VIF                      (26)
          }
        }
        priority 1 restrict srcip {                                            (27)
          entry-id 1 {                                                         (28)
            match flow-list IPV6_LIST3                                         (29)
            action redirect                                                    (30)
            redirect-destination vnode VEX4 interface VIF                      (31)
          }
        }
      }
    }
  }
  vexternal VEX2 {                                                              (32)
    ofs-map ofs-datapath-id 0002-0002-0002-0002 ofs-port GBE0/2 vlan-id 4095   (33)
    interface VIF                                                               (34)
  }
  vexternal VEX3 {                                                              (35)
    ofs-map ofs-datapath-id 0003-0003-0003-0003 ofs-port GBE0/3 vlan-id 4095   (36)
    interface VIF                                                               (37)
  }
  vexternal VEX4 {                                                              (38)
    ofs-map ofs-datapath-id 0004-0004-0004-0004 ofs-port GBE0/4 vlan-id 4095   (39)
    interface VIF                                                               (40)
  }
}
```

[Description]

Table 3-8   Description of Commands

Number	Description
(1)	Create a flow list with the name IPV6_LIST1. Specify the ipv6 option. Use the restrict option to set available match conditions to srcip and ip-proto.
(2) to (3)	For sequence-number 1, specify a match condition for source IPv6 address 2001:100::1/64 and protocol number 58 (ICMPv6). Unspecified fields are considered as ANY (all matches).
(4)	Create a flow list with the name IPV6_LIST2. Specify the ipv6 option. Use the restrict option to set available match conditions to srcip and dstip.
(5) to (7)	For sequence-number 1, specify a match condition for destination IPv6 address fffe::1/64 and source IPv6 address 2001:100::1/64. Unspecified fields are considered as ANY (all matches).
(8)	Create a flow list with the name IPV6_LIST3. Specify the ipv6 option. Use the restrict option to set available match conditions to srcip.
(9) to (11)	For sequence-number 1, specify a match condition for source IPv6 address 2001:100::1/64. Unspecified fields are considered as ANY (all matches).
(12)	Create a VTN with the name VTN1.
(13)	Create a vExternal with the name VEX1.
(14)	Map an OFS port to VEX1. Specify VLAN ID=4095, which represents VLAN ANY.
(15) to (16)	Create a virtual interface VIF for VEX1. Apply the safe flow filter to VIF.
(17)	For priority 3, set the available match conditions to srcip and ip-proto.
(18) to (21)	For entry-id 1, define flow list IPV6_LIST1 as a match condition and set its action to redirect. Specify VIF in VEX2 for a vExternal virtual interface to redirect.
(22)	For priority 2, set the available match conditions to srcip and dstip.
(23) to (26)	For entry-id 1, define flow list IPV6_LIST2 as a match condition and set its action to redirect. Specify VIF in VEX3 for a vExternal virtual interface to redirect.
(27)	For priority 1, set the available match conditions to srcip.
(28) to (31)	For entry-id 1, define flow list IPV6_LIST3 as a match condition and set its action to redirect. Specify VIF in VEX4 for a vExternal virtual interface to redirect.
(32)	Create a vExternal with the name VEX2.
(33)	Map an OFS port to VEX2. Specify VLAN ID=4095, which represents VLAN ANY.
(34)	Create a virtual interface VIF for VEX2.

Number	Description
(35)	Create a vExternal with the name VEX3.
(36)	Map an OFS port to VEX3. Specify VLAN ID=4095, which represents VLAN ANY.
(37)	Create a virtual interface VIF for VEX3.
(38)	Create a vExternal with the name VEX4.
(39)	Map an OFS port to VEX4. Specify VLAN ID=4095, which represents VLAN ANY.
(40)	Create a virtual interface VIF for VEX4.

[Example of Overall Configuration]

```
network-default {
  openflow-version 1.3
  vtn-station aging-time 60
}
real-network {
  ofs 1 {
    datapath 0001-0001-0001-0001
    port "GBE0/1" {
      external-port
    }
  }
  ofs 2 {
    datapath 0002-0002-0002-0002
    port "GBE0/2" {
      external-port
    }
  }
  ofs 3 {
    datapath 0003-0003-0003-0003
    port "GBE0/3" {
      external-port
    }
  }
  ofs 4 {
    datapath 0004-0004-0004-0004
    port "GBE0/4" {
      external-port
    }
  }
  port-group enable
}
flow-list IPV6_LIST1 ipv6 restrict srcip ip-proto {
  sequence-number 1 {
    ip-protocol 58
    ipv6 ip-source-address 2001:100::1/128
  }
}
flow-list IPV6_LIST2 ipv6 restrict srcip dstip {
  sequence-number 1 {
    ipv6 ip-destination-address fffe::1/128
    ipv6 ip-source-address 2001:100::1/128
  }
}
flow-list IPV6_LIST3 ipv6 restrict srcip {
  sequence-number 1 {
    ipv6 ip-source-address 2001:100::1/128
  }
}
vtn VTN1 {
  vexternal VEX1 {
    ofs-map ofs-datapath-id 0001-0001-0001-0001 ofs-port GBE0/1 vlan-id 4095
    interface VIF {
      flow-filter-safe {
        priority 3 restrict srcip ip-proto {
          entry-id 1 {
            match flow-list IPV6_LIST1
            action redirect
            redirect-destination vnode VEX2 interface VIF
          }
        }
        priority 2 restrict srcip dstip {
          entry-id 1 {
            match flow-list IPV6_LIST2
            action redirect
            redirect-destination vnode VEX3 interface VIF
          }
        }
        priority 1 restrict srcip {
          entry-id 1 {
            match flow-list IPV6_LIST3
            action redirect
            redirect-destination vnode VEX4 interface VIF
          }
        }
      }
    }
  }
  vexternal VEX2 {
    ofs-map ofs-datapath-id 0002-0002-0002-0002 ofs-port GBE0/2 vlan-id 4095
    interface VIF
  }
  vexternal VEX3 {
    ofs-map ofs-datapath-id 0003-0003-0003-0003 ofs-port GBE0/3 vlan-id 4095
    interface VIF
  }
  vexternal VEX4 {
    ofs-map ofs-datapath-id 0004-0004-0004-0004 ofs-port GBE0/4 vlan-id 4095
    interface VIF
  }
}
```

PF6800 Ver. 6.1
PFTAP User's Guide

PFC00EY0610-01

January, 2015 1st Edition

NEC Corporation