

---

*AX8600R Software Manual*

**Configuration Guide Vol. 2**  
**For Version 12.1**

AX86R-S002X

**Alaxala**

## ■ Relevant products

This manual applies to the models in the AX8600R series of devices. It also describes the functionality of version 12.1 of the software for the AX8600R series of devices.

## ■ Export restrictions

In the event that any or all ALAXALA products (including technologies, programs and services) described or contained herein are controlled under any of applicable export control laws and regulations (including the Foreign Exchange and Foreign Trade Law of Japan and United States export control laws and regulations), such products shall not be exported without obtaining the required export licenses from the authorities concerned in accordance with the above laws.

## ■ Trademarks

Cisco is a registered trademark of Cisco Systems, Inc. in the United States and other countries.

Ethernet is a registered trademark of Xerox Corporation.

IPX is a trademark of Novell, Inc.

sFlow is a registered trademark of InMon Corporation in the United States and other countries.

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

Other company and product names in this document are trademarks or registered trademarks of their respective owners.

## ■ Reading and storing this manual

Before you use the equipment, carefully read the manual and make sure that you understand all safety precautions.

After reading the manual, keep it in a convenient place for easy reference.

## ■ Notes

Information in this document is subject to change without notice.

## ■ Editions history

August 2013 (Edition 1) AX86R-S002X

## ■ Copyright

All Rights Reserved, Copyright(C), 2012, 2013, ALAXALA Networks, Corp.

---

# Preface

---

## Applicable products and software versions

This manual applies to the models in the AX8600R series of devices. It also describes the functionality of version 12.1 of the software for the AX8600R series of devices.

Before you operate the equipment, carefully read the manual and make sure that you understand all instructions and cautionary notes. After reading the manual, keep it in a convenient place for easy reference.

## Corrections to the manual

Corrections to this manual might be contained in the *Release Notes* and *Manual Corrections* that come with the software.

## Intended readers

This manual is intended for system administrators who wish to configure and operate a network system that uses the Device.

Readers must have an understanding of the following:

- The basics of network system management

## Manual URL

You can view this manual on our website at:

<http://www.alaxala.com/en/>

## Reading sequence of the manuals

The following shows the manuals you need to consult according to your requirements determined from the following workflow for installing, setting up, and starting regular operation of the Device.

- **Unpacking the Device and the basic settings for initial installation**

Quick Start Guide

(AX86R-Q001X)

- **Determining the hardware setup requirements and how to handle the hardware**

Hardware Instruction Manual

(AX86R-H001X)

- **Understanding the software functions, configuration settings, and operation commands**

▽ First, see the following guides to check the functions or capacity limits.

- |                                      |                      |                        |
|--------------------------------------|----------------------|------------------------|
| - Capacity limits                    | - Filters and QoS    | - IP packet forwarding |
| - Basic operations (e.g. logging in) | - Network management | - Unicast routing      |
| - Ethernet                           |                      | - Multicast routing    |

Configuration Guide Vol. 1

(AX86R-S001X)

Configuration Guide Vol. 2

(AX86R-S002X)

Configuration Guide Vol. 3

(AX86R-S003X)

▽ If necessary, see the following references.

- **Learning the syntax of commands and the details of command parameters**

Configuration Command Reference Vol. 1

(AX86R-S004X)

Configuration Command Reference Vol. 2

(AX86R-S005X)

Configuration Command Reference Vol. 3

(AX86R-S006X)

Operation Command Reference Vol. 1

(AX86R-S007X)

Operation Command Reference Vol. 2

(AX86R-S008X)

Operation Command Reference Vol. 3

(AX86R-S009X)

- **Understanding system messages and logs**

Message and Log Reference

(AX86R-S010X)

- **Understanding MIBs**

MIB Reference

(AX86R-S011X)

- **How to troubleshoot when a problem occurs**

Troubleshooting Guide

(AX86R-T001X)

## Conventions: The terms "Device" and "device"

The term Device (upper-case "D") is an abbreviation for the following:

AX8600R series device

The term device (lower-case "d") might refer to a Device, another type of device from the current vendor, or a device from another vendor. The context decides the meaning.

## Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit

BEQ	Best Effort Queueing
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second (can also appear as bps)
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CC	Continuity Check
CCM	Continuity Check Message
CFM	Connectivity Fault Management
CFP	C Form-factor Pluggable
CIDR	Classless Inter-Domain Routing
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
E-mail	Electronic mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ETH-AIS	Ethernet Alarm Indicator Signal
ETH-LCK	Ethernet Locked Signal
FAN	Fan Unit
FCS	Frame Check Sequence
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ	Low Latency Queueing
LSA	Link State Advertisement
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEG	Maintenance Entity Group
MEP	Maintenance association End Point/Maintenance entity group End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MP	Maintenance Point

MRU	Maximum Receive Unit
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NBMA	Non-Broadcast Multiple-Access
NDP	Neighbor Discovery Protocol
NIF	Network Interface
NLA ID	Next-Level Aggregation Identifier
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PA	Protocol Accelerator
packet/s	packets per second (can also appear as pps)
PAD	PADding
PC	Personal Computer
PDU	Protocol Data Unit
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PQ	Priority Queueing
PRU	Packet Routing Unit
PS	Power Supply
PSINPUT	Power Supply Input
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RR	Round Robin
RQ	ReQuest
SA	Source Address
SD	Secure Digital
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	Small Form factor Pluggable Plus
SFU	Switch Fabric Unit
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
uRPF	unicast Reverse Path Forwarding
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
RRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

WFQ	Weighted Fair Queueing
WWW	World-Wide Web

## **Conventions: KB, MB, GB, and TB**

This manual uses the following conventions: 1 KB (kilobyte) is  $1024$  bytes. 1 MB (megabyte) is  $1024^2$  bytes. 1 GB (gigabyte) is  $1024^3$  bytes. 1 TB (terabyte) is  $1024^4$  bytes.





---

# Contents

---

<b>Preface</b>	<b>i</b>
Applicable products and software versions .....	i
Corrections to the manual .....	i
Intended readers .....	i
Manual URL .....	i
Reading sequence of the manuals .....	i
Conventions: The terms "Device" and "device" .....	ii
Abbreviations used in the manual .....	ii
Conventions: KB, MB, GB, and TB .....	v

## **PART 1: Filters**

<b>1. Filters</b>	<b>1</b>
1.1 Description .....	2
1.1.1 Overview of filters .....	2
1.1.2 Flow detection .....	3
1.1.3 Flow detection mode .....	3
1.1.4 Flow detection conditions .....	4
1.1.5 Access lists .....	8
1.1.6 Implicit discarding .....	9
1.1.7 Notes on using the filter .....	10
1.2 Configuration .....	12
1.2.1 List of configuration commands .....	12
1.2.2 Configuring the flow detection mode .....	12
1.2.3 Configuring frame forwarding and discarding by MAC header .....	13
1.2.4 Configuring frame forwarding and discarding by IP header and TCP/UDP header ..	13
1.2.5 Configuring frame forwarding and discarding by MAC header, IP header, and TCP/UDP header .....	15
1.2.6 Configuring filters for multiple interface .....	17
1.3 Operation .....	18
1.3.1 List of operation commands .....	18
1.3.2 Checking filters .....	18

## **PART 2: QoS**

<b>2. Overview of QoS</b>	<b>21</b>
2.1 Structure of QoS control .....	22
2.2 Configuration common to QoS control .....	23
2.2.1 List of configuration commands .....	23
2.3 Operations common to QoS control .....	25
2.3.1 List of operation commands .....	25
<b>3. QoS Flow</b>	<b>27</b>
3.1 Description .....	28
3.1.1 Overview .....	28
3.1.2 Flow detection .....	28
3.1.3 Flow detection mode .....	29
3.1.4 Flow detection conditions .....	29
3.1.5 QoS flow lists .....	34

3.1.6	Notes on using flow detection .....	35
3.2	Configuration .....	37
3.2.1	List of configuration commands .....	37
3.2.2	Configuring the flow detection mode .....	37
3.2.3	Configuring a QoS flow for multiple interface .....	38
3.3	Operation .....	39
3.3.1	List of operation commands .....	39
3.3.2	Checking the QoS flow operation when IPv4 packets are set as the flow detection condition .....	39
<b>4.</b>	<b>Policer</b> .....	<b>41</b>
4.1	Description .....	42
4.1.1	Overview .....	42
4.1.2	Aggregate policer .....	44
4.1.3	Notes on using the policer .....	44
4.2	Configuration .....	46
4.2.1	List of configuration commands .....	46
4.2.2	Configuring maximum bandwidth monitoring .....	46
4.2.3	Configuring a discard class for non-compliant minimum bandwidth monitoring .....	47
4.2.4	Configuring DSCP rewrite for non-compliant minimum bandwidth monitoring .....	48
4.2.5	Configuring the combined use of maximum bandwidth monitoring and minimum bandwidth monitoring .....	49
4.2.6	Configuring maximum bandwidth monitoring with an aggregate policer .....	50
4.3	Operation .....	52
4.3.1	List of operation commands .....	52
4.3.2	Checking the details of maximum bandwidth monitoring .....	52
4.3.3	Checking discard class for non-compliant minimum bandwidth monitoring .....	52
4.3.4	Checking DSCP rewrite when non-compliance occurs in minimum monitoring bandwidth .....	53
4.3.5	Checking the combined use of maximum bandwidth monitoring and minimum bandwidth monitoring .....	54
4.3.6	Checking the details of maximum bandwidth monitoring with an aggregate policer .....	55
<b>5.</b>	<b>Marker</b> .....	<b>57</b>
5.1	Description .....	58
5.1.1	User priority rewrite .....	58
5.1.2	DSCP rewrite .....	58
5.1.3	Notes on using the marker .....	59
5.2	Configuration .....	60
5.2.1	List of configuration commands .....	60
5.2.2	Configuring user priority rewrite .....	60
5.2.3	Configuring DSCP rewrite .....	61
5.3	Operation .....	62
5.3.1	List of operation commands .....	62
5.3.2	Checking user priority rewrite .....	62
5.3.3	Checking DSCP rewrite .....	62
<b>6.</b>	<b>Priority Change</b> .....	<b>63</b>
6.1	Description .....	64
6.1.1	Direct specification of priority class and discard class .....	64
6.1.2	DSCP mapping .....	64
6.1.3	Notes on using priority change .....	65
6.2	Configuration .....	66
6.2.1	List of configuration commands .....	66
6.2.2	Configuring a priority class change .....	66
6.2.3	Configuring DSCP mapping .....	67

6.3	Operation .....	68
6.3.1	List of operation commands .....	68
6.3.2	Checking priority change .....	68
<b>7.</b>	<b>Port Shaper .....</b>	<b>69</b>
7.1	Description .....	70
7.1.1	Overview .....	70
7.1.2	Drop control .....	70
7.1.3	Scheduling .....	71
7.1.4	Queue number specification .....	73
7.1.5	Port bandwidth control .....	74
7.1.6	Notes on using the port shaper .....	75
7.2	Configuration .....	76
7.2.1	List of configuration commands .....	76
7.2.2	Configuring scheduling .....	76
7.2.3	Configuring queue number specification .....	76
7.2.4	Configuring port bandwidth control .....	77
7.2.5	Configuring queuing priority .....	77
7.3	Operation .....	79
7.3.1	List of operation commands .....	79
7.3.2	Checking scheduling .....	79
7.3.3	Checking queue number specification .....	79
7.3.4	Checking port bandwidth control .....	80
7.3.5	Checking queuing priority .....	80
7.4	Correspondence between NIFs and port shapers .....	82
<b>8.</b>	<b>Queues in the Device .....</b>	<b>83</b>
8.1	Description .....	84
8.1.1	Overview .....	84
8.2	Operation .....	86
8.2.1	List of operation commands .....	86
8.2.2	Checking BCU queue information .....	86
8.2.3	Checking PRU queue information .....	86
 <b>PART 3: Network Management</b>		
<b>9.</b>	<b>Port Mirroring .....</b>	<b>89</b>
9.1	Description .....	90
9.1.1	Overview of port mirroring .....	90
9.1.2	Port mirroring specifications .....	91
9.1.3	Notes on using port mirroring .....	91
9.2	Configuration .....	92
9.2.1	List of configuration commands .....	92
9.2.2	Configuring port mirroring .....	92
<b>10.</b>	<b>sFlow Statistics (Flow Statistics) Functionality .....</b>	<b>95</b>
10.1	Description .....	96
10.1.1	Overview of sFlow statistics .....	96
10.1.2	sFlow statistic agent functionality .....	97
10.1.3	sFlow packet format .....	97
10.1.4	Behavior of sFlow statistics on a Device .....	103
10.2	Configuration .....	106
10.2.1	List of configuration commands .....	106
10.2.2	Configuring basic settings for the sFlow statistics functionality .....	106
10.2.3	Configuration example for the sFlow statistics configuration parameter .....	109

10.3	Operation .....	113
10.3.1	List of operation commands .....	113
10.3.2	Checking communication with collectors .....	113
10.3.3	Checking the sFlow statistics during operation .....	113
10.3.4	Adjusting the sampling interval for sFlow statistics .....	114
<b>11.</b>	<b>CFM</b> .....	<b>115</b>
11.1	Description .....	116
11.1.1	Overview .....	116
11.1.2	CFM configuration elements .....	120
11.1.3	Designing domains .....	124
11.1.4	Continuity check .....	128
11.1.5	Loopback .....	131
11.1.6	Linktrace .....	132
11.1.7	ETH-AIS .....	135
11.1.8	ETH-LCK .....	135
11.1.9	Behavior for the port in the communication-blocked state .....	136
11.1.10	Databases used for CFM .....	136
11.1.11	Operation when connecting IEEE 802.1ag and ITU-T Y.1731 .....	138
11.1.12	Operation in BCU duplex configuration .....	138
11.1.13	Notes on using CFM .....	139
11.2	Configuration .....	140
11.2.1	List of configuration commands .....	140
11.2.2	Configuring IEEE 802.1ag CFM .....	140
11.2.3	Configuring ITU-T Y.1731 CFM .....	142
11.2.4	Configuration for using both IEEE 802.1ag and ITU-T Y.1731 .....	143
11.2.5	Stopping CFM on a port .....	144
11.3	Operation .....	145
11.3.1	List of operation commands .....	145
11.3.2	Checking connection between MPs .....	145
11.3.3	Checking the route between MPs .....	145
11.3.4	Checking the state of MPs on a route .....	146
11.3.5	Checking the CFM state .....	146
11.3.6	Checking detailed information of failures .....	146
<b>12.</b>	<b>LLDP</b> .....	<b>149</b>
12.1	Description .....	150
12.1.1	Overview .....	150
12.1.2	Supported specifications .....	150
12.1.3	Notes on using LLDP .....	151
12.2	Configuration .....	152
12.2.1	List of configuration commands .....	152
12.2.2	Configuring LLDP .....	152
12.3	Operation .....	153
12.3.1	List of operation commands .....	153
12.3.2	Displaying LLDP information .....	153
<b>Appendix</b>	.....	<b>155</b>
A	Relevant standards .....	156
A.1	Policer .....	156
A.2	Marker .....	156
A.3	Diff-serv .....	156
A.4	sFlow .....	156
A.5	CFM .....	156
A.6	LLDP .....	157





## **Chapter**

---

# **1. Filters**

---

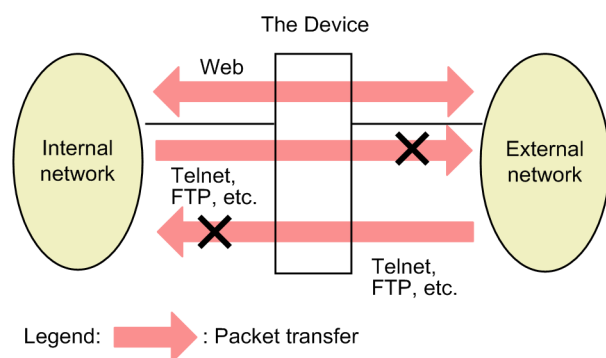
Filter functionality is used to forward and discard received frames and sent frames. This chapter provides an overview of the filter functionality and describes how to use it.

- 1.1 Description
- 1.2 Configuration
- 1.3 Operation

## 1.1 Description

Filters are functionality used for forwarding or discarding certain types of received frames or sent frames. It is used to strengthen network security. You can use filters to limit access to the network by user or by protocol. For example, you can forward Web data between an internal network and an external network while at the same time discarding any Telnet and FTP data to prevent unauthorized access from the external network and leakage of information to the external network from the internal network. The following figure shows an example of network configuration that uses filters.

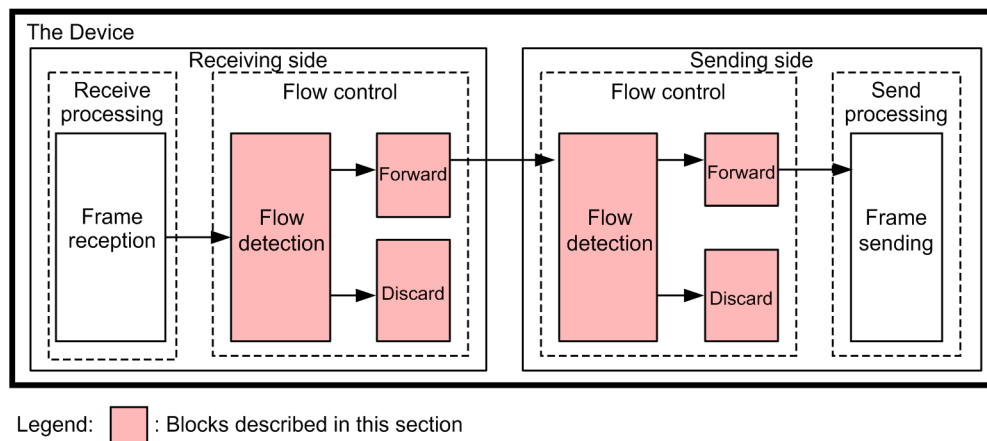
Figure 1-1: Example of network configuration using filters



### 1.1.1 Overview of filters

The following figure shows the functional blocks for filters on the Device.

Figure 1-2: Functional blocks for filters



The following table describes an overview of the functional blocks shown in the figure.

Table 1-1: Overview of functional blocks for filters

Section and functional blocks		Overview of authentication VLAN functionality
Flow control	Flow detection	Detects a flow (specific frames) that matches a condition, such as MAC address, protocol type, IP address, or TCP/UDP port number.
	Forward and discard	Forwards and discards frames found by the flow detection block.

To use a filter on a Device, you need to create a filter entry that defines a combination of flow



detection condition (such as MAC address, protocol type, IP address, or TCP/UDP port number) and an operation (forward or discard).

The following describes how a filter works on the Device:

1. The filter entries set for each interface are searched in the order of priority specified by the user.
2. The search terminates when the filter entry matching the frame is found.
3. Whether the frame is forwarded or discarded is determined according to the operation specified for the filter entry.
4. If the frame does not match any filter entry, the frame is discarded. For details about discard operations, see *1.1.6 Implicit discarding*.

### 1.1.2 Flow detection

The flow detection functionality detects a flow, which is a sequence of frames, based on conditions, such as the MAC header, IP header, and TCP header. Settings are configured in access lists. For details about access lists, see *1.1.5 Access lists*.

The following table describes availability of flow detection and access list settings for each interface in the Device.

*Table 1-2: Availability of flow detection and access list settings for each interface*

Interface	Flow detection	Setting the access lists
Ethernet interface	Y	Y
Ethernet subinterface	Y	Y
Port channel interface	Y <sup>#</sup>	--
Port channel subinterface	Y	Y
Loopback interface	--	--
Null interface	--	--
Management port	--	--
AUX port	--	--

Legend: Y: Available, --: Not available

<sup>#</sup>

Flow detection is available if you set an access list to the Ethernet interfaces for which the channel group is configured.

### 1.1.3 Flow detection mode

The Device provides flow detection modes for determination of flow detection operation. The following describes the features of each flow detection mode.

#### Quantity-oriented mode

More entries can be used but the detection condition is restricted as follows:

- The MAC header is used for the flow detection for non-IP packets.
- The combination of the IP header and Layer 4 header is used for the flow detection for IP packets.

#### Detection-condition-oriented mode

Less entries are used but more detailed detection is possible because the number of detection

conditions per entry can increase. Advanced detection condition, which is the combination of the MAC header, IP header, and Layer 4 header, is used for the flow detection to target both non-IP and IP packets.

Flow detection mode can be specified by using the `flow detection mode configuration` command. By default, the Device is set to quantity-oriented mode. For details about flow detection modes and flow detection operations, see *1.1.5 Access lists*.

### 1.1.4 Flow detection conditions

To perform flow detection, specify the conditions for identifying the flow in the configuration. Flow detection conditions can be sorted into MAC conditions, IPv4 conditions, IPv6 conditions, and Advance conditions. The following table describes the flow detection conditions and corresponding detectable headers.

*Table 1-3: Flow detection conditions and corresponding detectable headers*

Flow detection conditions	MAC header	VLAN tag header	IPv4 header	IPv6 header	Layer 4 header
MAC conditions	Y	Y	--	--	--
IPv4 conditions	--	Y	Y	--	Y
IPv6 conditions	--	Y	--	Y	Y
Advance conditions	Y	Y	Y	Y	Y

Legend: Y: Can be detected, --: Cannot be detected

The following table describes the detailed items that can be specified in each flow detection condition.

*Table 1-4: Detailed items that can be specified in each flow detection condition*

Type		Configuration items	
MAC conditions	MAC header	Source MAC address	
		Destination MAC address	
		Ethernet type	
	VLAN tag header <sup>#1</sup>	VLAN ID of the tag	
		User priority	
		Without a tag	
IPv4 conditions	VLAN tag header <sup>#1</sup>	User priority	
		Without a tag	
	IPv4 header	Upper layer protocol	
		Source IP address	
		Destination IP address	
		ToS <sup>#2</sup>	
		DSCP <sup>#2</sup>	
		Precedence <sup>#2</sup>	
		Fragment <sup>#3</sup>	FO

Type		Configuration items	
			MF
		IP length	
	IPv4-TCP header	Source port number	
		Destination port number	
		TCP control flag <sup>#4</sup>	
	IPv4-UDP header	Source port number	
		Destination port number	
	IPv4-ICMP header	ICMP type	
		ICMP code	
	IPv4-IGMP header	IGMP type	
IPv6 conditions	VLAN tag header <sup>#1</sup>	User priority	
		Without a tag	
	IPv6 header	Upper layer protocol	
		Source IP address <sup>#5</sup>	
		Destination IP address	
		Traffic class <sup>#6</sup>	
		DSCP <sup>#6</sup>	
		Fragment <sup>#3</sup>	FO
			MF
		IP length	
	IPv6-TCP header	Source port number	
		Destination port number	
		TCP control flag <sup>#4</sup>	
	IPv6-UDP header	Source port number	
		Destination port number	
	IPv6-ICMP header	ICMP type	
		ICMP code	
Advance conditions	MAC header	Source MAC address <sup>#7</sup>	
		Destination MAC address	
		Ethernet type	
	VLAN tag header <sup>#1</sup>	VLAN ID of the tag	
		User priority	
		Without a tag	

## 1. Filters

Type		Configuration items	
	IPv4 header	Upper layer protocol	
		Source IP address	
		Destination IP address	
		ToS <sup>#2</sup>	
		DSCP <sup>#2</sup>	
		Precedence <sup>#2</sup>	
		Fragment <sup>#3</sup>	FO
			MF
		IP length	
	IPv4-TCP header	Source port number	
		Destination port number	
		TCP control flag <sup>#4</sup>	
	IPv4-UDP header	Source port number	
		Destination port number	
	IPv4-ICMP header	ICMP type	
		ICMP code	
	IPv4-IGMP header	IGMP type	
	IPv6 header	Upper layer protocol	
		Source IP address	
		Destination IP address	
		Traffic class <sup>#6</sup>	
		DSCP <sup>#6</sup>	
		Fragment <sup>#3</sup>	FO
			MF
		IP length	
	IPv6-TCP header	Source port number	
		Destination port number	
		TCP control flag <sup>#4</sup>	
	IPv6-UDP header	Source port number	
		Destination port number	
	IPv6-ICMP header	ICMP type	
		ICMP code	

#1

The following describes how the detection works if you specify the VLAN tag header:

VLAN ID of the tag

The VLAN ID of the VLAN tag header. The untagged frames are not detected.

User priority

The user priority in VLAN tag header is used for detection. The untagged frames are not detected.

Without a tag

Untagged frames are detected. The tagged frames are not detected.

#2

The following describes how the detection works if you specify the ToS field:

ToS

Value of bits 3 to 6 in the ToS field.

Precedence

Value of the three highest-order bits in the ToS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			ToS			-	

DSCP

Value of the six highest-order bits in the ToS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

#3

The following describes how the detection works if you specify the fragment parameter. If `+fo` is specified, only VLAN tag header and IP header can be specified for flow detection condition.

`+fo`

A fragmented packet in the middle and the last fragmented packet are detected.

`-fo`

A non-fragmented packet and the first fragmented packet are detected.

`+mf`

The first fragmented packet and a fragmented packet in the middle are detected.

`-mf`

A non-fragmented packet and the last fragmented packet are detected.

The following table describes the relationship between the combination of the fragment parameters and packets to be detected.

*Table 1-5:* Relationship between the combination of the fragment parameters and packets to be detected

Fragment parameter		Non-fragmented packets	Fragmented packets		
FO	MF		First	Middle	Last
Not specified	Not specified	Y	Y	Y	Y
	-mf	Y	--	--	Y
	+mf	--	Y	Y	--
-fo	Not specified	Y	Y	--	--
	-mf	Y	--	--	--
	+mf	--	Y	--	--
+fo	Not specified	--	--	Y	Y
	-mf	--	--	--	Y
	+mf	--	--	Y	--

Legend: Y: Detected, --: Not detected

#4

ack, fin, psh, rst, syn, and urg flags are detected.

#5

Only the 64 highest-order bits can be specified.

#6

The following describes how the detection works if you specify the traffic class field:

Traffic class

Value for the traffic class field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Traffic class							

DSCP

Value of the six highest-order bits in the traffic class field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

#7

If you specify the source MAC address as a detection condition at the sending-side interface, the Device that will forward the packets detects the source MAC address when the Device receives the packets.

### 1.1.5 Access lists

To perform flow detection for the filter, set access lists in the configuration. The access list that you need to set depends on the flow detection conditions. The type of detectable frames also depends on the flow detection conditions. The following table describes the relationship between the flow detection conditions, access lists, and types of frames to be detected.

*Table 1-6:* Relationship between the flow detection conditions, access lists, and types of frames to be detected

Flow detection conditions	Access lists	Types of frames to be detected					
		Quantity-oriented mode			Detection-condition-oriented mode		
		Non-IP	IPv4	IPv6	Non-IP	IPv4	IPv6
MAC conditions	mac access-list	Y	--	--	Y	--	--
IPv4 conditions	ip access-list	--	Y	--	--	Y	--
IPv6 conditions	ipv6 access-list	--	--	Y	--	--	Y
Advance conditions	advance access-list	--#	--#	--#	Y	Y	Y

Legend: Y: Detected, --: Not detected

#

In quantity-oriented mode, you cannot apply Advance conditions to the interface.

Use the access list group command and IPv6 traffic filter command to apply an access list to an interface.

Note that in the flow detection, the application order of the access list items is determined by the specified conditions. The following describes the application order for the flow detection under each specified condition.

### **(1) Order within an access list**

If multiple filter entries are set in an access list, the Device detects the frames according to the ascending order of the sequence number for the filter entries.

### **(2) Order within the same interface**

If multiple access lists are set in the same interface, the Device detects the frames according to the following order:

1. The MAC access list, IPv4 access list, or IPv6 access list
2. The Advance access list

For example, if a frame is detected in flow detection by the MAC access list, that frame is not detected in flow detection by the Advance access list. The frame is not counted in statistics, either.

### **(3) Order for multiple interfaces**

If you set an access list to the Ethernet interface and Ethernet subinterface to which the target Ethernet interface belongs or port channel subinterface, frames are detected in the following order:

1. Ethernet interface
2. The Ethernet subinterface or port channel subinterface

## **1.1.6 Implicit discarding**

Frames that do not match any flow detection conditions are discarded on an interface where a filter is specified. This is called implicit discarding.

The implicit discard entries are automatically generated for each access list. The frames to be detected by the preceding access list always match either the filter entry or the implicit discard entry. For this reason, no frames are detected in flow detection by access lists that are later in the flow detection order.

If no access lists are set, all frames are forwarded.

### (1) Order within the same interface

The following describes the flow detection order within the same interface.

1. The MAC access list, IPv4 access list, or IPv6 access list
2. The Advance access list

If a MAC access list and an Advance access list are specified in the same interface, the frames detected by the MAC access list always match the filter entry or the implicit discard entry. For this reason, no frames are detected in flow detection by the Advance access list.

### (2) Order for multiple interfaces

The following describes the flow detection order for multiple interfaces:

1. Ethernet interface
2. The Ethernet subinterface or port channel subinterface

If you set the access list to the Ethernet interface and the Ethernet subinterface to which the target Ethernet interface belongs, the frames detected by the access list set to the Ethernet interface always match either the filter entry or the implicit discard entry. Therefore, the frames are not detected in flow detection by the access list set to the Ethernet subinterface.

## 1.1.7 Notes on using the filter

### (1) Filters for IPv6 packets that have an ESP extension header

To perform flow detection for IPv6 packets that have an ESP extension header, specify the following headers in the flow detection conditions:

- MAC header
- VLAN tag header
- IPv6 header

Even if you specify TCP, UDP, and ICMP headers in the flow detection condition, they are not detected.

### (2) Filters for fragmented IPv4 packets

Fragmented packets after the first one do not have a TCP, UDP, ICMP, or the IGMP header. The following table describes how the filter works when the Device receives fragmented packets.

Table 1-7: Relationship between fragmented packets and the filter

Flow detection conditions	Match between flow detection conditions and packets	Operation	First packet	Following packets
Only IP header	IP header matches.	Forward	Forward	Forward
		Discard	Discard	Discard
	IP header does not match.	Forward	Searches for the next entry.	Searches for the next entry.
		Discard	Searches for the next entry.	Searches for the next entry.



Flow detection conditions	Match between flow detection conditions and packets	Operation	First packet	Following packets
IP header + TCP, UDP, ICMP, or the IGMP header	IP header matches. TCP, UDP, ICMP, or IGMP header matches.	Forward	Forward	--
		Discard	Discard	--
	IP header matches. TCP, UDP, ICMP, and IGMP headers do not match.	Forward	Searches for the next entry.	Searches for the next entry.
		Discard	Searches for the next entry.	Searches for the next entry.
	IP header does not match. TCP, UDP, ICMP, and IGMP headers do not match.	Forward	Searches for the next entry.	Searches for the next entry.
		Discard	Searches for the next entry.	Searches for the next entry.

#### Legend

--: Not applicable because the packets do not have a TCP, UDP, ICMP, or IGMP header. The packets are always treated as having no match in a TCP, UDP, ICMP, or IGMP header.

### (3) Operation when filter entries are deleted

If you delete the filter entry during the following configuration changes, frames are temporarily discarded by the implicit discard entry:

- Deleting an access list with one or more entries set by the access group commands from the interface
- Deleting the last filter entry from the access list that is already applied to the interface by the access group command.

### (4) Operation when filter entries are changed

If a filter entry applied to an interface is changed on the Device, detectable frames are detected by other filter entries or by the implicit discard entry until the change is applied.

Also, if the updated filter entry is a flow detection condition that includes multiple entries, collection of statistics starts after all the filter entries are applied to the Device.

### (5) Frames that are not detected by filter

In the Device, the following frames are not detected in flow detection by the filters set at the receiving side:

- Frames discarded by uRPF

In the Device, the following frames are not detected in flow detection by the filter set at the sending side:

- Frames copied by port mirroring

## 1.2 Configuration

### 1.2.1 List of configuration commands

The following table describes the configuration commands for filters.

*Table 1-8: List of configuration commands*

Command name	Description
advance access-group	Applies the Advance filter functionality to an interface by setting an Advance filter with Advance conditions to the interface.
advance access-list	Sets an access list to serve as an Advance filter.
advance access-list resequence	Resets the sequence number for the order in which the filter conditions in an Advance filter are applied.
deny	Specifies the condition by which the filter discards frames.
ip access-group	Sets an IPv4 filter to an interface and enables the IPv4 filter functionality.
ip access-list extended	Sets an access list to serve as an IPv4 packet filter.
ip access-list resequence	Re-sequences the sequence numbers that determine the order in which the IPv4 address filter and IPv4 packet filter apply filter conditions.
ip access-list standard	Sets an access list to serve as an IPv4 address filter.
ipv6 access-list	Sets an access list to serve as an IPv6 filter.
ipv6 access-list resequence	Re-sequences the sequence numbers that determine the order in which the IPv6 filter applies filter conditions.
ipv6 traffic-filter	Sets an IPv6 filter to an interface and enables the IPv6 filter functionality.
mac access-group	Sets a MAC filter to an interface and enables the MAC filter functionality.
mac access-list extended	Sets an access list to serve as a MAC filter.
mac access-list resequence	Resets the sequence number for the order in which the filter conditions in a MAC filter are applied.
permit	Specifies the condition by which the filter forwards frames.
remark	Specifies supplementary information for the filter.
flow detection mode <sup>#</sup>	Sets the flow detection mode for the filter and QoS flow.
flow-table allocation <sup>#</sup>	Sets the distribution pattern of the filter and QoS flow.

#

See 9. *Device Management* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

### 1.2.2 Configuring the flow detection mode

The following shows an example of setting the flow detection mode to detection-condition-oriented mode.

#### Points to note

By default, the flow detection mode of the Device is set to quantity-oriented mode. Restart all the PRUs to apply the specified flow detection mode.

### Command examples

#### 1. **(config)# flow detection mode condition-oriented**

In global configuration mode, sets the flow detection mode to detection-condition-oriented mode.

### Notes

- Quantity-oriented mode can be changed if no Advance access list or Advance QoS flow list is specified for any of the interfaces.
- Detection-condition-oriented mode can be changed if the number of entries in the filter or QoS flow is within the capacity limit.

## 1.2.3 Configuring frame forwarding and discarding by MAC header

The following shows an example of specifying frame forwarding and discarding based on the MAC header as the flow detection condition.

### Points to note

When frames are received, flow detection is performed based on the MAC header. The frames that match the filter entry are either discarded or forwarded.

### Command examples

#### 1. **(config)# mac access-list extended IPX\_DENY**

Creates a MAC access-list (IPX\_DENY). After creating the list, the command switches to MAC filtering mode.

#### 2. **(config-ext-macl)# deny any any ipx**

Sets a MAC filter that discards frames whose Ethernet type is IPX.

#### 3. **(config-ext-macl)# permit any any**

Sets a MAC filter that forwards all frames.

#### 4. **(config-ext-macl)# exit**

Returns to global configuration mode from MAC filtering mode.

#### 5. **(config)# interface gigabitethernet 1/1**

Switches to configuration command mode for Ethernet interface 1/1.

#### 6. **(config-if)# mac access-group IPX\_DENY in**

Applies the MAC filter on the receiving side.

## 1.2.4 Configuring frame forwarding and discarding by IP header and TCP/UDP header

### (1) *Using IPv4 address as the flow detection condition*

The following shows an example of specifying frame forwarding and discarding based only on the IPv4 address as the flow detection condition.

### Points to note

When frames are received, flow detection is performed based on only the source IPv4 address. The frames that match the filter entry are forwarded. All IP packets that do not match the filter entry are discarded.

#### Command examples

1. **(config)# ip access-list standard FLOOR\_A\_PERMIT**  
Creates an IP access-list (FLOOR\_A\_PERMIT). After creating the list, the command switches to IPv4 address filtering mode.
2. **(config-std-nacl)# permit 192.0.2.0 0.0.0.255**  
Sets an IPv4 address filter that forwards the frames from the source IP address 192.0.2.0/24 network.
3. **(config-std-nacl)# exit**  
Returns to global configuration mode from IPv4 address filtering mode.
4. **(config)# interface gigabitethernet 1/1.10**  
Switches to configuration command mode for Ethernet subinterface 1/1.10.
5. **(config-subif)# ip access-group FLOOR\_A\_PERMIT in**  
Applies the IPv4 address filter on the receiving side.

### ***(2) Using IPv4 packet as the flow detection condition***

The following shows an example of specifying frame forwarding and discarding based on specification of IPv4 HTTP packet as the flow detection condition.

#### Points to note

When frames are received, flow detection is performed based on the IP header and TCP/UDP header, and the frames that match the filter entry are discarded.

#### Command examples

1. **(config)# ip access-list extended HTTP\_DENY**  
Creates an IP access-list (HTTP\_DENY). After creating the list, the command switches to IPv4 packet filtering mode.
2. **(config-ext-nacl)# deny tcp any any eq http**  
Sets an IPv4 packet filter that discards HTTP packets.
3. **(config-ext-nacl)# permit ip any any**  
Sets an IPv4 packet filter that forwards all frames.
4. **(config-ext-nacl)# exit**  
Returns to global configuration mode from IPv4 address filtering mode.

5. **(config)# interface port-channel 10.10**

Switches to configuration command mode for port channel subinterface 10.10.

6. **(config-subif)# ip access-group HTTP\_DENY in**

Applies the IPv4 packet filter to the receiving side.

### **(3) Using IPv6 packet as the flow detection conditions**

The following shows an example of specifying frame forwarding and discarding based on specification of IPv6 packet as the flow detection condition.

Points to note

When frames are received, flow detection is performed based on the IPv6 address. The frames that match the filter entry are forwarded. All IPv6 packets that do not match the filter entry are discarded.

Command examples

1. **(config)# ipv6 access-list FLOOR\_B\_PERMIT**

Creates an IPv6 access-list (FLOOR\_B\_PERMIT). After creating the list, the command switches to IPv6 filtering mode.

2. **(config-ipv6-acl)# permit ipv6 2001:db8::/32 any**

Sets an IPv6 filter that forwards frames from source IP address 2001:db8::/32.

3. **(config-ipv6-acl)# exit**

Returns to global configuration mode from IPv6 filtering mode.

4. **(config)# interface gigabitethernet 1/1**

Switches to configuration command mode for Ethernet interface 1/1.

5. **(config-if)# ipv6 traffic-filter FLOOR\_B\_PERMIT in**

Applies the IPv6 filter on the receiving side.

## **1.2.5 Configuring frame forwarding and discarding by MAC header, IP header, and TCP/UDP header**

### **(1) Using the MAC header, IPv4 header, and TCP header as the flow detection condition**

The following shows an example of specifying frame forwarding and discarding based on MAC header, IPv4 header, and TCP header as the flow detection condition.

Points to note

When frames are received, flow detection is performed based on the source MAC address, source IPv4 address, and TCP header. The frames that match the filter entry are forwarded. All frames that do not match the filter entry are discarded.

Command examples

1. **(config)# advance access-list ADVANCE\_ACL\_A\_PERMIT**  
Creates an Advance access-list (ADVANCE\_ACL\_A\_PERMIT). After creating the list, the command switches to Advance filtering mode.
2. **(config-adv-acl)# permit mac-ip host 0012.e200.0001 any tcp 192.0.2.0 0.0.0.255 any eq http**  
Sets an Advance filter that forwards HTTP packets from the source MAC address 0012.e200.0001 and the source IP address 192.0.2.0/24.
3. **(config-adv-acl)# exit**  
Returns to global configuration mode from Advance filtering mode.
4. **(config)# interface gigabitethernet 1/1.10**  
Switches to configuration command mode for Ethernet subinterface 1/1.10.
5. **(config-subif)# advance access-group ADVANCE\_ACL\_A\_PERMIT in**  
Applies the Advance filter on the receiving side.

## ***(2) Using the MAC header, IPv6 header, and UDP header as the flow detection condition***

The following shows an example of specifying frame forwarding and discarding based on the MAC header, IPv6 header, and UDP header as the flow detection condition.

### **Points to note**

When frames are received, flow detection is performed based on the source MAC address, source IPv6 address, and UDP header. The frames that match the filter entry are forwarded. All frames that do not match the filter entry are discarded.

### **Command examples**

1. **(config)# advance access-list ADVANCE\_ACL\_B\_PERMIT**  
Creates an Advance access-list (ADVANCE\_ACL\_B\_PERMIT). After creating the list, the command switches to Advance filtering mode.
2. **(config-adv-acl)# permit mac-ipv6 host 0012.e200.0001 any udp 2001:db8::/32 any eq ntp**  
Sets an Advance filter that forwards NTP packets from the source MAC address 0012.e200.0001 and the source IP address 2001:db8::/32.
3. **(config-adv-acl)# exit**  
Returns to global configuration mode from Advance filtering mode.
4. **(config)# interface port-channel 10.10**  
Switches to configuration command mode for port channel subinterface 10.10.

5. **(config-subif)# advance access-group ADVANCE\_ACL\_B\_PERMIT in**  
Applies the Advance filter on the receiving side.

## 1.2.6 Configuring filters for multiple interface

The following shows an example of setting a filter on multiple Ethernet interfaces.

Points to note

A filter can be set for multiple Ethernet interfaces in config-if-range mode.

Command examples

1. **(config)# ip access-list standard FLOOR\_C\_PERMIT**  
Creates an IP access-list (FLOOR\_C\_PERMIT). After creating the list, the command switches to IPv4 address filtering mode.
2. **(config-std-nacl)# permit 192.0.2.0 0.0.0.255**  
Sets an IPv4 address filter that forwards the frames from the source IP address 192.0.2.0/24 network.
3. **(config-std-nacl)# exit**  
Returns to global configuration mode from IPv4 address filtering mode.
4. **(config)# interface range gigabitethernet 1/1-4**  
Switches to configuration command mode for Ethernet interface 1/1-4.
5. **(config-if-range)# ip access-group FLOOR\_C\_PERMIT in**  
Applies the IPv4 address filter on the receiving side.

## 1.3 Operation

### 1.3.1 List of operation commands

The following table describes the operation commands for filters.

*Table 1-9: List of operation commands*

Command name	Description
show access-filter	Shows the filter setting details and statistics.
clear access-filter	Clears the filter statistics.
restart filter-qosflow <sup>#</sup>	Restarts the filter and QoS flow control program.
dump filter-qosflow <sup>#</sup>	Outputs the control information collected by the filter and QoS flow control program to a file.

#

See 4. *Common to Filters and QoS* in the manual *Operation Command Reference Vol. 2 For Version 12.1*.

### 1.3.2 Checking filters

You can check the filter operations by using the `show access-filter` command. To check the operation of filters for multiple interfaces, specify the range of interfaces.

#### (1) Checking the entries set for an Ethernet interface

The following figure shows how to check operation when a filter is set for an Ethernet interface.

*Figure 1-3: Checking operation when a filter is set for an Ethernet interface*

```
> show access-filter interface gigabitethernet 1/1 IPX_DENY in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 in
Extended MAC access-list : IPX_DENY
  10 deny any any ipx(0x8137)
      Matched packets      Matched bytes
Total   :                74699826      4780788864
PRU 1   :                74699826      4780788864
  20 permit any any
      Matched packets      Matched bytes
Total   :                718235      45967040
PRU 1   :                718235      45967040
Implicit-deny
      Matched packets      Matched bytes
Total   :                0      0
PRU 1   :                0      0
```

Make sure that `Extended MAC access-list` is displayed for the filter of the specified Ethernet interface. You can check the frames that match the flow detection condition by checking the value of `Matched packets` for `Matched bytes`. Also, you can check the frames that match the implicit discard entry by checking the value of `Matched packets` for `Matched bytes` fields under `Implicit-deny`.

#### (2) Checking the entries set for a port channel subinterface

The following figure shows how to check the operation when a filter is set for a port channel subinterface.

*Figure 1-4: Checking the operation when a filter is set for a port channel subinterface*



```

> show access-filter interface port-channel 10.10 HTTP_DENY in
Date 20XX/01/01 12:00:00 UTC
Using interface: port-channel 10.10 in
Extended IP access-list: HTTP_DENY
  10 deny tcp(6) any any eq http(80)
      Matched packets      Matched bytes
    Total :                1052789      161801506
    PRU 1 :                 894321      151659506
    PRU 3 :                 158468      10142000
  20 permit ip any any
      Matched packets      Matched bytes
    Total :               100535750      15476889608
    PRU 1 :               74699826      11653172856
    PRU 3 :               25835924       3823716752
Implicit-deny
      Matched packets      Matched bytes
    Total :                  0              0
    PRU 1 :                  0              0
    PRU 3 :                  0              0

```

Make sure that Extended IP access-list is displayed for the filter of the specified port channel subinterface. You can check the frames that match the flow detection condition by checking the value of Matched packets for Matched bytes. Also, you can check the frames that match the implicit discard entry by checking the value of Matched packets for Matched bytes fields under Implicit-deny.



## **Chapter**

---

# **2. Overview of QoS**

---

The QoS functionality provides a policer, a marker, priority changes, and bandwidth control as means of controlling the quality of communications and ensuring the efficient use of limited network resources, such as line bandwidth and queue buffer capacity. This chapter describes QoS control on the Device.

- 2.1 Structure of QoS control
- 2.2 Configuration common to QoS control
- 2.3 Operations common to QoS control

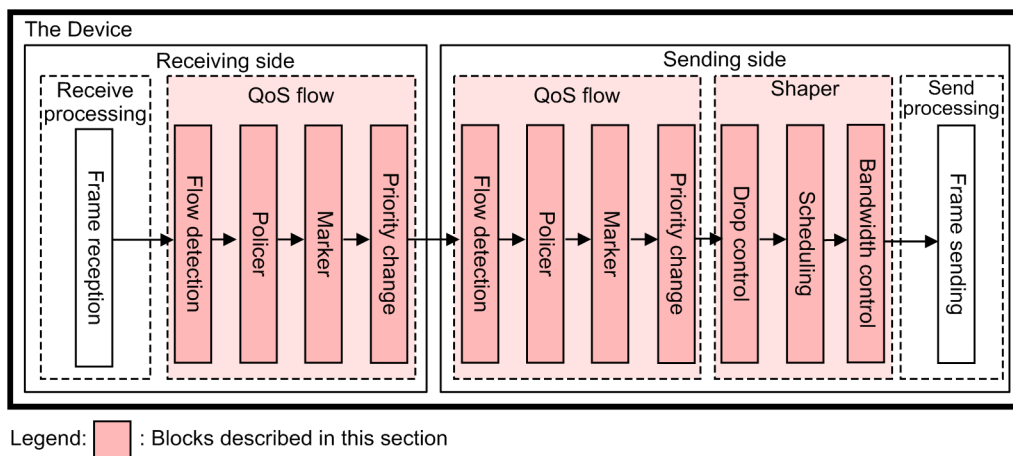
## 2.1 Structure of QoS control

Along with best-effort traffic that does not require guaranteed communications quality, the growing diversification of network services has meant an increase in real-time and guaranteed bandwidth traffic. You can use QoS control on the Device to provide communications quality appropriate for the type of traffic.

QoS control on the Device ensures the efficient use of limited network resources, such as line bandwidth and queue buffer capacity. To satisfy the many types of communications quality required for applications, use QoS control to distribute network resources in the most appropriate manner.

The following figure shows the functional blocks for QoS control on the Device.

Figure 2-1: Functional blocks for QoS control on the Device



The following table describes an overview of the functional blocks shown in the figure.

Table 2-1: Overview of functional blocks for QoS control

Section and functional blocks		Overview
QoS flow	Flow detection	Detects a flow that matches a condition, such as a MAC header, protocol type, IP address, or port number.
	Policer	Monitors the bandwidth of frame flow and assigns a penalty to frames that exceed the bandwidth.
	Marker	Updates the user priority in the VLAN tag header or the DSCP in the IP header.
	Priority change	Changes the priority class and the discard class for flows that indicates how easily a frame can be discarded.
Shaper	Drop control	Controls whether frames can be queued or discarded according to the priority of the frames and queue status.
	Scheduling	Controls the output order of frames from queues.
	Bandwidth control	Controls the output bandwidth of the ports.

In the QoS flow, the policer, the marker, and priority changes are applied to the detected flow.

In the shaper, drop control, scheduling, and the bandwidth control at the time of sending are applied based on the priority of the frame.

## 2.2 Configuration common to QoS control

### 2.2.1 List of configuration commands

The following table describes the configuration commands for QoS control.

*Table 2-2: List of configuration commands*

Command name	Description
advance qos-flow-group	Sets an Advance QoS flow list to an interface and applies QoS control based on Advance conditions.
advance qos-flow-list	Sets the Advance QoS flow list that is used for the flow detection based on Advance conditions.
advance qos-flow-list resequence	Re-sets the sequence number for the order in which the conditions in the Advance QoS flow list are applied.
ip qos-flow-group	Applies an IPv4 QoS flow list to an interface and enables IPv4 QoS control.
ip qos-flow-list	Sets the QoS flow list used for IPv4 QoS flow detection.
ip qos-flow-list resequence	Re-sets the sequence number for the order in which the conditions in the IPv4 QoS flow list are applied.
ipv6 qos-flow-group	Applies an IPv6 QoS flow list to an interface and enables IPv6 QoS control.
ipv6 qos-flow-list	Sets the QoS flow list used for IPv6 QoS flow detection.
ipv6 qos-flow-list resequence	Re-sets the sequence number for the order in which the conditions in the IPv6 QoS flow list are applied.
mac qos-flow-group	Applies a MAC QoS flow list to an interface and enables MAC QoS control.
mac qos-flow-list	Sets the QoS flow list used for MAC QoS flow detection.
mac qos-flow-list resequence	Re-sets the sequence number for the order in which the conditions in the MAC QoS flow list are applied.
policer	Sets the policer entry to be specified in the QoS flow list.
qos	Specifies the flow detection conditions and action specifications in the QoS flow list.
qos-queue-group	Applies a QoS queue list to an Ethernet interface and enables the shaper.
qos-queue-list	Sets the scheduling and queue number specification to the QoS queue list that stores the port shaper settings.
remark	Specifies supplementary information for QoS.
traffic-shape rate	Sets the port bandwidth control for port shaper to an Ethernet interface.
flow detection mode <sup>#</sup>	Sets the flow detection mode for the filter and QoS flow.
flow-table allocation <sup>#</sup>	Sets the distribution pattern of the filter and QoS flow.

#

See 9. *Device Management* in the manual *Configuration Command Reference Vol. 1 For*

*Version 12.1.*

## 2.3 Operations common to QoS control

### 2.3.1 List of operation commands

The following table describes the operation commands common to QoS control.

*Table 2-3: List of operation commands*

Command name	Description
show qos-flow	Shows the QoS flow setting details and statistics.
clear qos-flow	Clears the QoS flow statistics.
show policer	Shows the policer setting details and statistics.
clear policer	Clears the policer statistics.
show qos queueing	Shows all the queue information in the Device.
clear qos queueing	Clears all the queue statistics that are displayed by using the <code>show qos queueing</code> command.
show qos queueing bcu	Shows BCU queue information.
clear qos queueing bcu	Clears all the queue statistics that are displayed by using the <code>show qos queueing bcu</code> command.
show qos queueing pru	Shows PRU queue information.
clear qos queueing pru	Clears all the queue statistics that are displayed by using the <code>show qos queueing pru</code> command.
show qos queueing port	Shows information about the port input and output queues.
clear qos queueing port	Clears all the queue statistics that are displayed by using the <code>show qos queueing port</code> command.
restart queue-control	Restarts the queue control program to which the shaper is to be set.
dump queue-control	Outputs to a file the control information collected by the queue control program to which the shaper is to be set.
restart filter-qosflow <sup>#</sup>	Restarts the filter and QoS flow control program to which the QoS flow is to be set.
dump filter-qosflow <sup>#</sup>	Outputs to a file the control information collected by the filter and QoS flow control program to which the QoS flow is to be set.

#

See 4. *Common to Filters and QoS* in the manual *Operation Command Reference Vol. 2 For Version 12.1*.





## Chapter

---

# 3. QoS Flow

---

The QoS flow functionality is used to apply a policer, a marker, and priority changes to the frames detected in flow detection. This chapter provides an overview of the flow detection in the QoS flow and describes how to use it.

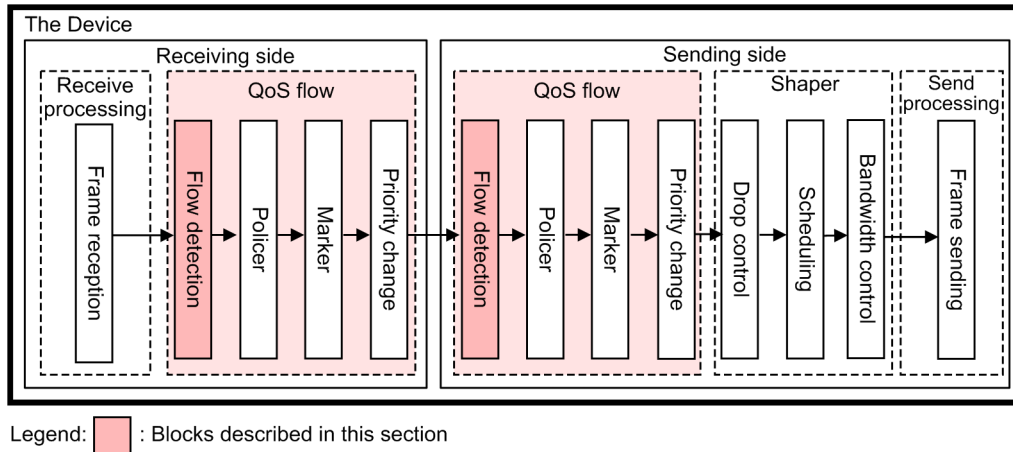
- 3.1 Description
- 3.2 Configuration
- 3.3 Operation

## 3.1 Description

### 3.1.1 Overview

The QoS flow is functionality to apply a policer, a marker, and priority changes to the certain types of receive frames or send frames. The following figure shows the positioning of the functional block for the QoS flow and flow detection in the Device.

Figure 3-1: Positioning of the functional block for the QoS flow and flow detection in the Device



### 3.1.2 Flow detection

The flow detection functionality detects a flow, which is a sequence of frames, based on conditions, such as the MAC header, IP header, and TCP header. QoS flow lists are used to set up flow detection. For details about the QoS flow lists, see 3.1.5 *QoS flow lists*.

The following table describes availability of flow detection and the QoS flow list settings for each interface in the Device.

Table 3-1: Availability of flow detection and the QoS flow list settings for each interface

Interface	Flow detection	QoS flow list settings
Ethernet interface	Y	Y
Ethernet subinterface	Y	Y
Port channel interface	Y <sup>#</sup>	--
Port channel subinterface	Y	Y
Loopback interface	--	--
Null interface	--	--
Management port	--	--
AUX port	--	--

Legend: Y: Can be detected or set, --: Cannot be detected or set

#

Flow detection is available if you set a QoS flow list to the Ethernet interfaces for which the channel group is configured.

### 3.1.3 Flow detection mode

The Device provides flow detection modes for determination of flow detection operation. The following describes the features of each flow detection mode.

#### Quantity-oriented mode

More entries can be used but the detection condition is restricted as follows:

- The MAC header is used for the flow detection for non-IP packets.
- The combination of the IP header and Layer 4 header is used for the flow detection for IP packets.

#### Detection-condition-oriented mode

Less entries are used but more detailed detection is possible because the number of detection conditions per entry can increase. Advanced detection condition, which is the combination of the MAC header, IP header, and Layer 4 header, is used for the flow detection to target both non-IP and IP packets.

Flow detection mode can be specified by using the `flow detection mode configuration` command. By default, the Device is set to quantity-oriented mode. For details about flow detection modes and flow detection operations, see 3.1.5 *QoS flow lists*.

### 3.1.4 Flow detection conditions

To perform flow detection, specify the conditions for identifying the flow in the configuration. Flow detection conditions can be sorted into MAC conditions, IPv4 conditions, IPv6 conditions, and Advance conditions. The following table describes the flow detection conditions and corresponding detectable headers.

Table 3-2: Flow detection conditions and corresponding detectable headers

Flow detection conditions	MAC header	VLAN tag header	IPv4 header	IPv6 header	Layer 4 header
MAC conditions	Y	Y	--	--	--
IPv4 conditions	--	Y	Y	--	Y
IPv6 conditions	--	Y	--	Y	Y
Advance conditions	Y	Y	Y	Y	Y

Legend: Y: Can be detected, --: Cannot be detected

The following table describes the detailed items that can be specified in each flow detection condition.

Table 3-3: Detailed items that can be specified in each flow detection condition

Type		Configuration items
MAC conditions	MAC header	Source MAC address
		Destination MAC address
		Ethernet type
	VLAN tag header <sup>#1</sup>	VLAN ID of the tag
		User priority
		Without a tag
IPv4 conditions	VLAN tag header <sup>#1</sup>	User priority

Type		Configuration items	
	IPv4 header	Without a tag	
		Upper layer protocol	
		Source IP address	
		Destination IP address	
		ToS <sup>#2</sup>	
		DSCP <sup>#2</sup>	
		Precedence <sup>#2</sup>	
		Fragment <sup>#3</sup>	FO
			MF
		IP length	
	IPv4-TCP header	Source port number	
		Destination port number	
		TCP control flag <sup>#4</sup>	
	IPv4-UDP header	Source port number	
		Destination port number	
	IPv4-ICMP header	ICMP type	
		ICMP code	
	IPv4-IGMP header	IGMP type	
IPv6 conditions	VLAN tag header <sup>#1</sup>	User priority	
		Without a tag	
	IPv6 header	Upper layer protocol	
		Source IP address <sup>#5</sup>	
		Destination IP address	
		Traffic class <sup>#6</sup>	
		DSCP <sup>#6</sup>	
		Fragment <sup>#3</sup>	FO
			MF
		IP length	
	IPv6-TCP header	Source port number	
		Destination port number	
		TCP control flag <sup>#4</sup>	
	IPv6-UDP header	Source port number	
		Destination port number	

Type		Configuration items	
Advance conditions	IPv6-ICMP header	ICMP type	
		ICMP code	
	MAC header	Source MAC address <sup>#7</sup>	
		Destination MAC address	
		Ethernet type	
	VLAN tag header <sup>#1</sup>	VLAN ID of the tag	
		User priority	
		Without a tag	
	IPv4 header	Upper layer protocol	
		Source IP address	
		Destination IP address	
		ToS <sup>#2</sup>	
		DSCP <sup>#2</sup>	
		Precedence <sup>#2</sup>	
		Fragment <sup>#3</sup>	FO
			MF
		IP length	
	IPv4-TCP header	Source port number	
		Destination port number	
		TCP control flag <sup>#4</sup>	
	IPv4-UDP header	Source port number	
		Destination port number	
	IPv4-ICMP header	ICMP type	
		ICMP code	
	IPv4-IGMP header	IGMP type	
	IPv6 header	Upper layer protocol	
		Source IP address	
		Destination IP address	
		Traffic class <sup>#6</sup>	
		DSCP <sup>#6</sup>	
		Fragment <sup>#3</sup>	FO
			MF
		IP length	

Type		Configuration items
	IPv6-TCP header	Source port number
		Destination port number
		TCP control flag <sup>#4</sup>
	IPv6-UDP header	Source port number
		Destination port number
	IPv6-ICMP header	ICMP type
		ICMP code

#1

The following describes how the detection works if you specify the VLAN tag header:

The VLAN ID of the tag

The VLAN ID of the VLAN tag header. The untagged frames are not detected.

User priority

The user priority in the VLAN tag header. The untagged frames are not detected.

Without a tag

The untagged frames are detected. The tagged frames are not detected.

#2

The following describes how the detection works if you specify the ToS field:

ToS

Value of bits 3 to 6 in the ToS field.

Precedence

Value of the three highest-order bits in the ToS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			ToS			-	

DSCP

Value of the six highest-order bits in the ToS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

#3

The following describes how the detection works if you specify the fragment parameter. If +fo is specified, only VLAN tag header and IP header can be specified for flow detection condition.

+fo

A fragmented packet in the middle and the last fragmented packet are detected.

-fo

A non-fragmented packet and the first fragmented packet are detected.

+mf

The first fragmented packet and a fragmented packet in the middle are detected.

-mf

A non-fragmented packet and the last fragmented packet are detected.

The following table describes the relationship between the combination of the fragment parameters and packets to be detected.

*Table 3-4:* Relationship between the combination of the fragment parameters and packets to be detected

Fragment parameter		Non-fragmented packets	Fragmented packets		
FO	MF		First	Middle	Last
Not specified	Not specified	Y	Y	Y	Y
	-mf	Y	--	--	Y
	+mf	--	Y	Y	--
-fo	Not specified	Y	Y	--	--
	-mf	Y	--	--	--
	+mf	--	Y	--	--
+fo	Not specified	--	--	Y	Y
	-mf	--	--	--	Y
	+mf	--	--	Y	--

Legend: Y: Detected, --: Not detected

#4

ack, fin, psh, rst, syn, and urg flags are detected.

#5

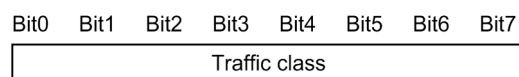
Only the 64 highest-order bits can be specified.

#6

The following describes how the detection works if you specify the traffic class field:

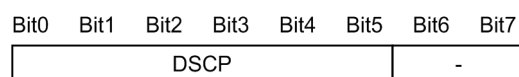
Traffic class

Value is for the traffic class field.



DSCP

Value of the six highest-order bits in the traffic class field.



#7

If you specify the source MAC address as a detection condition at the sending-side interface, the Device that will forward the packets detects the source MAC address when the Device

receives the packets.

### 3.1.5 QoS flow lists

To perform QoS flow detection, set a QoS flow list in the configuration. The QoS flow list to be set differs according to the flow detection condition. The type of frame that can be detected differs depending on the flow detection condition. The following table describes the relationship between the flow detection conditions, QoS flow lists, and types of frames to be detected.

*Table 3-5: Relationship between the flow detection conditions, QoS flow lists, and types of frames to be detected*

Flow detection conditions	QoS flow list	Types of frames to be detected					
		Quantity-oriented mode			Detection-condition-oriented mode		
		Non-IP	IPv4	IPv6	Non-IP	IPv4	IPv6
MAC conditions	mac qos-flow-list	Y	--	--	Y	--	--
IPv4 conditions	ip qos-flow-list	--	Y	--	--	Y	--
IPv6 conditions	ipv6 qos-flow-list	--	--	Y	--	--	Y
Advance conditions	advance qos-flow-list	--#	--#	--#	Y	Y	Y

Legend: Y: Detected, --: Not detected

#

In quantity-oriented mode, you cannot apply Advance conditions to the interface.

Use a QoS flow group command to apply the QoS flow lists to an interface.

Note that, for a QoS flow list, the order in which flow detection occurs depends on the specified conditions. The following describes the order in which flow detection occurs under each specified condition.

#### (1) Order within a QoS flow list

If multiple QoS flow entries are set in a QoS flow list, the Device detects the frames according to the ascending order of the sequence number for the QoS flow entries.

#### (2) Order within the same interface

If multiple QoS flow lists are set in the same interface, the Device detects the frames according to the following order:

1. The MAC QoS flow list, IPv4 QoS flow list, or IPv6 QoS flow list
2. The Advance QoS flow list

For example, if a frame is detected in flow detection by the MAC QoS flow list, that frame is not detected in flow detection by the Advance QoS flow list. The frame is not counted in statistics, either.

#### (3) Order in multiple interfaces

If you set a QoS flow list to the Ethernet interface and Ethernet subinterface to which the target Ethernet interface belongs or port channel subinterface, frames are detected in the following order.

1. Ethernet interface
2. Ethernet subinterface or port channel subinterface



### 3.1.6 Notes on using flow detection

#### (1) QoS flow detection for IPv6 packets that have an ESP extension header

To perform QoS flow detection for IPv6 packets that have an ESP extension header, specify the following headers in the flow detection conditions:

- MAC header
- VLAN tag header
- IPv6 header

Even if you specify TCP, UDP, and ICMP headers in flow detection conditions, IPv6 packets with ESP extension header are not detected by the QoS flow detection.

#### (2) QoS flow detection for fragmented packets

Fragmented packets after the first one do not have a TCP, UDP, ICMP, or IGMP header. The following table describes how QoS flow detection works when the Device receives fragmented packets.

Table 3-6: Relationship between fragmented packets and QoS flow detection

Flow detection conditions	Match between flow detection conditions and packets	First packet	Following packets
Only IP header	IP header matches.	Operates according to the matched entry.	Operates according to the matched entry.
	IP header does not match.	Searches for the next entry.	Searches for the next entry.
IP header + TCP, UDP, ICMP, or IGMP header	IP header matches. TCP, UDP, ICMP, or IGMP header matches.	Operates according to the matched entry.	--
	IP header matches. TCP, UDP, ICMP, and IGMP headers do not match.	Searches for the next entry.	Searches for the next entry.
	IP header does not match. TCP, UDP, ICMP, and IGMP headers do not match.	Searches for the next entry.	Searches for the next entry.

Legend

--: Not applicable because the packets do not have a TCP, UDP, ICMP, or IGMP header. The packets are always treated as having no match in a TCP, UDP, ICMP, or IGMP header.

#### (3) Operation when a QoS flow entry is changed

If a QoS flow entry applied to an interface is changed on the Device, detectable frames might be detected by other QoS flow entries until the change is applied.

Also, if the updated QoS flow entry is a flow detection condition that includes multiple entries, collection of statistics starts after all the QoS flow entries are applied to the Device.

#### (4) Frames that are not detected by the QoS flow detection

In the Device, the following frames are not detected in flow detection by the QoS flow set at the receiving side:

- Frames discarded by uRPF
- Frames discarded by the filter settings on the receiving side
- Packets discarded by a null interface

- Packets discarded because the direct broadcast forwarding is disabled
- Packets discarded by the unicast forwarding functionality at packet receipt
- Packets discarded by the multicast forwarding functionality at packet receipt
- Packets discarded by policy-based routing at packet receipt
- Frames sent to the Device
- IPv4 packets whose TTL is set to 1
- IPV6 packets whose hop limit is set to 1

Furthermore, the following frames are not detected in flow detection by the QoS flow set at the sending side:

- Frames discarded by the filter settings on the sending side
- Frames copied by port mirroring

## 3.2 Configuration

### 3.2.1 List of configuration commands

The following table describes the configuration commands for a QoS flow.

*Table 3-7: List of configuration commands*

Command name	Description
advance qos-flow-group	Sets an Advance QoS flow list to an interface and applies QoS control based on Advance conditions.
advance qos-flow-list	Sets the Advance QoS flow list that is used for the flow detection based on Advance conditions.
advance qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the Advance QoS flow list are applied.
ip qos-flow-group	Applies an IPv4 QoS flow list to an interface and enables IPv4 QoS control.
ip qos-flow-list	Sets the QoS flow list used for IPv4 QoS flow detection.
ip qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv4 QoS flow list are applied.
ipv6 qos-flow-group	Applies an IPv6 QoS flow list to an interface and enables IPv6 QoS control.
ipv6 qos-flow-list	Sets the QoS flow list used for IPv6 QoS flow detection.
ipv6 qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv6 QoS flow list are applied.
mac qos-flow-group	Applies a MAC QoS flow list to an interface and enables MAC QoS control.
mac qos-flow-list	Sets the QoS flow list used for MAC QoS flow detection.
mac qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the MAC QoS flow list are applied.
qos	Specifies flow detection conditions and action specifications in the QoS flow list.
remark	Specifies supplementary information for QoS.
flow detection mode <sup>#</sup>	Sets the flow detection mode for the filter and QoS flow.
flow-table allocation <sup>#</sup>	Sets the distribution pattern of the filter and QoS flow.

#

See 9. *Device Management* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

### 3.2.2 Configuring the flow detection mode

The following shows an example of setting the flow detection mode to detection-condition-oriented mode.

#### Points to note

By default, the flow detection mode of the Device is set to quantity-oriented mode. Restart all the PRUs to apply the specified flow detection mode.

#### Command examples

1. **(config)# flow detection mode condition-oriented**

In global configuration mode, sets the flow detection mode to detection-condition-oriented mode.

#### Notes

- Quantity-oriented mode can be changed if no Advance access list or Advance QoS flow list is specified for any of the interfaces.
- Detection-condition-oriented mode can be changed if the number of entries in the filter or QoS flow is within the capacity limit.

### 3.2.3 Configuring a QoS flow for multiple interface

The following example shows how to set a QoS flow on multiple Ethernet interfaces.

#### Points to note

A QoS flow can be set for multiple Ethernet interfaces in config-if-range mode.

#### Command examples

1. **(config)# ip qos-flow-list QOS-LIST1**

Creates an IPv4 QoS flow list (QOS-LIST1). After creating the list, the command switches to IPv4 QoS flow list mode.

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action priority-class 6**

Configures the IPv4 QoS flow list in which the priority class is rewritten to 6 for flows whose destination IP address is 192.0.2.10.

3. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

4. **(config)# interface range gigabitethernet 1/1-4**

Switches to configuration command mode for Ethernet interface 1/1-4.

5. **(config-if-range)# ip qos-flow-group QOS-LIST1 out**

Applies the IPv4 QoS flow list on the sending side.

## 3.3 Operation

### 3.3.1 List of operation commands

The following table describes the operation commands for a QoS flow.

*Table 3-8:* List of operation commands

Command name	Description
show qos-flow	Shows the QoS flow setting details and statistics.
clear qos-flow	Clears the QoS flow statistics.

### 3.3.2 Checking the QoS flow operation when IPv4 packets are set as the flow detection condition

You can check the QoS flow operation by using the `show qos-flow` command. To check the operation of the QoS flow for multiple interfaces, specify the range of interfaces.

The following figure shows how to check the QoS flow operation when IPv4 packets are set as the flow detection condition.

*Figure 3-2:* Checking the QoS flow operation when IPv4 packets are set as the flow detection

```
> show qos-flow interface gigabitethernet 1/1 QOS-LIST1 out
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 out
IP qos-flow-list : QOS-LIST1
    10 ip any host 192.0.2.10 action priority-class 6
                Matched packets      Matched bytes
      Total   :                   5642          222540
      PRU 1   :                   5642          222540
>
```

Make sure that `IP qos-flow-list` is displayed for the QoS flow of the specified Ethernet interface. You can check the frames that match the flow detection condition by checking the value of Matched packets for Matched bytes.



## Chapter

---

# 4. Policer

---

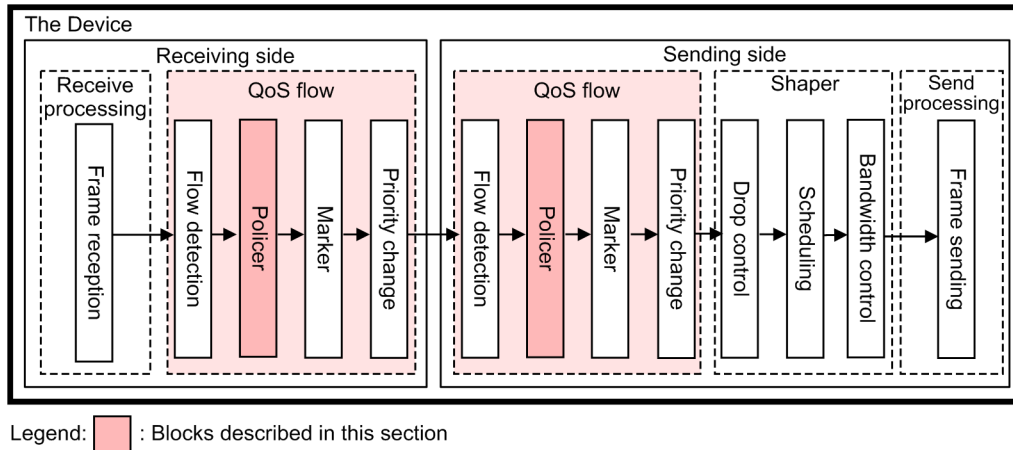
The policer functionality is used to monitor the bandwidth for the frames detected in flow detection by QoS flow. This chapter describes the policer and how to use it.

- 4.1 Description
- 4.2 Configuration
- 4.3 Operation

## 4.1 Description

The policer functionality is used to monitor the bandwidth for traffic flows subject to flow detection. The following figure shows the positioning of the policer block described in this section.

Figure 4-1: Positioning of the policer block



### 4.1.1 Overview

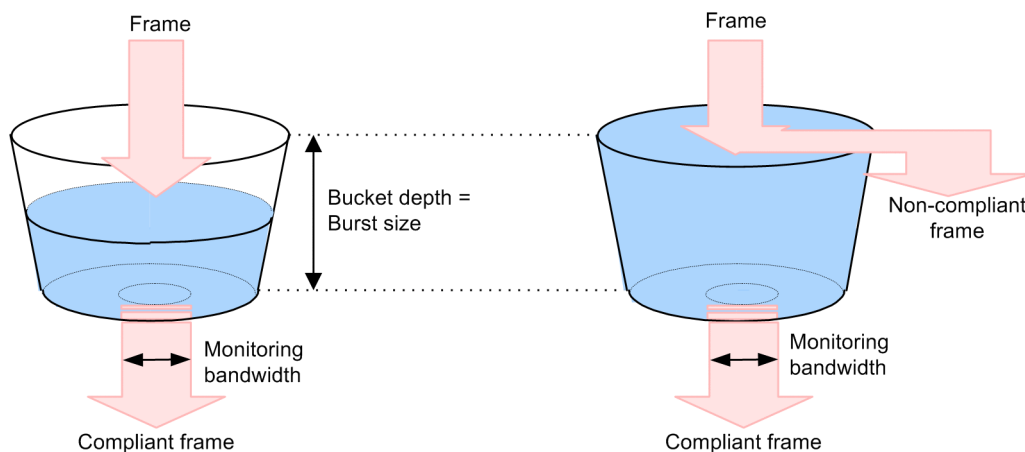
The policer monitors the bandwidth based on the frame length (from the inter-frame gap<sup>#</sup> to FCS) detected by flow detection. Frames that are forwarded as being within the specified monitoring bandwidth are referred to as compliant frames. Frames penalized for exceeding the monitoring bandwidth are referred to as non-compliant frames.

#: The inter-frame gap is 12 bytes.

The compliance of frames detected by flow detection with the monitoring bandwidth limit is determined by using the leaky bucket algorithm, the model for which is a bucket that contains water but has a hole in the bottom.

The following figure shows the model for the leaky bucket algorithm.

Figure 4-2: Model for the leaky bucket algorithm



Water leaks from the bucket at a constant rate that is the same as the monitoring bandwidth. When a frame is sent and received, water equivalent to the size from the inter-frame gap to FCS flows into the bucket. If the bucket does not overflow, the frame is forwarded as a compliant frame (the left example in the figure). If the bucket overflows, the frame is detected by flow detection as a



non-compliant frame and is penalized (the right example in the figure). The burst size refers to the amount of water that can be tolerated (that is, the depth of the bucket) when a large volume of water is temporarily added.

The bandwidth monitoring functionality consists of minimum bandwidth monitoring and maximum bandwidth monitoring. Minimum bandwidth monitoring uses the marker and priority change and updates the priority and the DSCP to penalize non-compliant frames. Maximum bandwidth monitoring simply discards non-compliant frames. The following table describes the types of penalties that can be used for minimum bandwidth monitoring and maximum bandwidth monitoring.

*Table 4-1: Types of penalties that can be used for minimum bandwidth monitoring and maximum bandwidth monitoring*

Penalty for non-compliant frames	Type of bandwidth monitoring	
	Minimum bandwidth monitoring	Maximum bandwidth monitoring
Discard	--	Y
Discard class change	Y	--
DSCP rewrite	Y	--
User priority rewrite	Y	--

Legend: Y: The penalty can be used, --: The penalty cannot be used.

If you use minimum and maximum bandwidth monitoring at the same time in a policer, you can use two-rate three-color or single-rate three-color policing depending on the combination of monitoring bandwidth value and burst size.

### **(1) Two-rate three-color policing**

In the two-rate three-color policing, frames are categorized and marked according to their size of bandwidth usage. The following table describes the categories of frames.

*Table 4-2: Categories of frames (two-rate three-color policing)*

Category	Color	Description
Non-compliant frame	Red	Frames that exceed the monitoring bandwidth value for maximum bandwidth monitoring
Exceeding frame	Yellow	Frames that exceed the monitoring bandwidth value for minimum bandwidth monitoring
Compliant frame	Green	Frames that are no more than the monitoring bandwidth value for minimum bandwidth monitoring

From among these, non-compliant frames (red) are discarded. Exceeding frames (yellow) are to be penalized according to the setting for the non-compliant frames in minimum bandwidth monitoring.

If you use the two-rate three-color policing, specify the monitoring bandwidth value for maximum bandwidth monitoring that is larger than that for minimum bandwidth monitoring.

### **(2) Single-rate three-color policing**

In the single-rate three-color policing, frames are categorized and marked according to their burstiness in certain bandwidth. The following table describes the categories of frames.

Table 4-3: Categories of frames (single-rate three-color policing)

Category	Color	Description
Non-compliant frame	Red	Frames that exceed the monitoring bandwidth value and the burst size for maximum bandwidth monitoring.
Exceeding frame	Yellow	Frames that exceed the monitoring bandwidth value and the burst size for minimum bandwidth monitoring.
Compliant frame	Green	Frames with the value no more than the monitoring bandwidth value.

From among these, non-compliant frames (red) are discarded. Exceeding frames (yellow) are to be penalized according to the setting for the non-compliant frames in minimum bandwidth monitoring.

If you use single-rate three-color policing, specify the same value for the monitoring bandwidth values for maximum bandwidth monitoring and minimum bandwidth monitoring. In addition, specify a burst size for maximum bandwidth monitoring that is larger than that for minimum bandwidth monitoring.

#### 4.1.2 Aggregate policer

The aggregate policer functionality monitors the bandwidth usage for multiple flows. This functionality can be used in both the receiving interface and the sending interface.

There are several ways to use the aggregate policer. You can specify the same policer entry to multiple QoS flow entries, or apply a QoS flow entry with a specified policer entry to multiple interfaces.

#### 4.1.3 Notes on using the policer

##### (1) Setting the burst size

To forward compliant packets in traffic that has large bandwidth fluctuations, specify a large value as the burst size.

Note that the value for the burst size must be larger than the frame length value for the flow detection. If the specified burst size value is smaller than the length of the inserted frame, the frame is sometimes determined as non-compliant even if the frame size is equal to or smaller than the specified bandwidth.

##### (2) Setting values for maximum and minimum bandwidth monitoring

If you set maximum and minimum bandwidth monitoring at the same time, and then specify the same value for the monitoring bandwidth value and burst size, the operation of the Device is the same as if you specified only the value for maximum bandwidth monitoring.

##### (3) Operation when the policer and other QoS flow functionality is used at the same time

If the policer is used with the marker and priority change, the Device prioritizes the operations in the following order and then sends the frames:

1. DSCP mapping set at the sending interface
2. Penalty for non-compliant frames found during minimum bandwidth monitoring set at the sending interface
3. Priority change or marker set at the sending interface
4. DSCP mapping set at the receiving interface
5. Penalty for non-compliant frames found during minimum bandwidth monitoring set at the receiving interface
6. Priority change or marker set at the receiving interface

**(4) Relationship between the policer specified for the traffic flow and the output line or output queue**

If you monitor the bandwidth by using the policer, specify the value for monitoring bandwidth within the bandwidth value of the output Ethernet interface or of the output queue for the target flow. If you use multiple policers for multiple flows, be careful of the total of the monitoring bandwidth values for each policer.

**(5) Policer for protocol control packets**

Protocol control frames are also subject to monitoring by the policer. Therefore, if a protocol control frame is found as a non-compliant frame in bandwidth monitoring, the frame is also penalized. You need to allocate the bandwidth while taking into account the size of the protocol control frame.

**(6) Using maximum bandwidth monitoring for TCP frames**

When you use maximum bandwidth monitoring, repeated slow startups of TCP might result in extremely slow data transfer rates.

To avoid this problem, use minimum bandwidth monitoring to specify an operation that lowers the discard class so that frames can be discarded more easily. This setting ensures that frames that exceed the contracted bandwidth are not discarded immediately.

**(7) Operations when setting a policer for multiple PRUs**

If you set a policer for multiple PRUs as in the following, the Device monitors bandwidth for each PRU:

- Applying the QoS flow, with a policer specified, to the port channel (subinterface) that consists of interfaces over multiple PRUs
- Applying the QoS flow, with a policer specified, to multiple interfaces that have different PRUs

## 4.2 Configuration

### 4.2.1 List of configuration commands

The following table describes the configuration commands for the policer.

*Table 4-4:* List of configuration commands

Command name	Description
advance qos-flow-group	Sets an Advance QoS flow list to an interface, and applies QoS control based on Advance conditions.
advance qos-flow-list	Sets the Advance QoS flow list that is used for flow detection based on Advance conditions.
advance qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the Advance QoS flow list are applied.
ip qos-flow-group	Applies an IPv4 QoS flow list to an interface and enables IPv4 QoS control.
ip qos-flow-list	Sets the QoS flow list used for IPv4 QoS flow detection.
ip qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv4 QoS flow list are applied.
ipv6 qos-flow-group	Applies an IPv6 QoS flow list to an interface and enables IPv6 QoS control.
ipv6 qos-flow-list	Sets the QoS flow list used for IPv6 QoS flow detection.
ipv6 qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv6 QoS flow list are applied.
mac qos-flow-group	Applies a MAC QoS flow list to an interface and enables MAC QoS control.
mac qos-flow-list	Sets the QoS flow list used for MAC QoS flow detection.
mac qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the MAC QoS flow list are applied.
policer	Sets the policer entry to be specified in the QoS flow list.
qos	Specifies flow detection conditions and action specifications in the QoS flow list.
remark	Specifies supplementary information for QoS.

### 4.2.2 Configuring maximum bandwidth monitoring

The following describes an example of performing maximum bandwidth monitoring for a certain type of flow.

#### Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then maximum bandwidth monitoring is performed.

#### Command examples

1. **(config)# policer POLICER-1 in max-rate 500M max-burst 100k**

Creates a policer entry (POLICER-1) and sets the values as follows:

- Monitoring bandwidth for maximum bandwidth monitoring: 500 Mbit/s

- Burst size for maximum bandwidth monitoring: 100 KB

2. **(config)# ip qos-flow-list QOS-LIST1**

Creates an IPv4 QoS flow list (QOS-LIST1). After creating the list, the command switches to IPv4 QoS flow list mode.

3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-1**

Configures the IPv4 QoS flow list in which the policer entry (POLICER-1) is specified for flows whose destination IP address is 192.0.2.10.

4. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

5. **(config)# interface gigabitethernet 1/1**

Switches to configuration command mode for Ethernet interface 1/1.

6. **(config-if)# ip qos-flow-group QOS-LIST1 in**

Applies the IPv4 QoS flow list (QOS-LIST1) to the receiving side.

### 4.2.3 Configuring a discard class for non-compliant minimum bandwidth monitoring

The following describes an example of performing minimum bandwidth monitoring for a certain type of flow and changing the discard class for non-compliant frames.

#### Points to note

When frames are sent, first flow detection is performed based on the destination IP address, and then minimum bandwidth monitoring is performed. The discard class of any non-compliant frames found during minimum bandwidth monitoring is changed.

#### Command examples

1. **(config)# policer POLICER-2 out min-rate 300M min-burst 80k penalty-discard-class 2**

Creates a policer entry (POLICER-2) and sets the values as follows:

- Monitoring bandwidth for minimum bandwidth monitoring: 300 Mbit/s
- Burst size for minimum bandwidth monitoring: 80 KB
- Discard class for non-compliant frames in minimum bandwidth monitoring: 2

2. **(config)# ip qos-flow-list QOS-LIST2**

Creates an IPv4 QoS flow list (QOS-LIST2). After creating the list, the command switches to IPv4 QoS flow list mode.

3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-2**

Configures the IPv4 QoS flow list in which the policer entry (`POLICER-2`) is specified for flows whose destination IP address is 192.0.2.10.

4. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

5. **(config)# interface gigabitethernet 1/3**

Switches to configuration command mode for Ethernet interface 1/3.

6. **(config-if)# ip qos-flow-group QOS-LIST2 out**

Applies the IPv4 QoS flow list (`QOS-LIST2`) to the sending side.

#### 4.2.4 Configuring DSCP rewrite for non-compliant minimum bandwidth monitoring

The following describes an example of performing minimum bandwidth monitoring for a certain type of flow and updating DSCP for non-compliant frames.

##### Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then minimum bandwidth monitoring is performed. The DSCP value of any non-compliant frames found during minimum bandwidth monitoring is changed.

##### Command examples

1. **(config)# policer POLICER-3 in min-rate 200M min-burst 70k penalty-dscp 11**

Creates a policer entry (`POLICER-3`) and sets the values as follows:

- Monitoring bandwidth for minimum bandwidth monitoring: 200 Mbit/s
- Burst size for minimum bandwidth monitoring: 70 KB
- DSCP value for non-compliant frames in minimum bandwidth monitoring: 11

2. **(config)# ip qos-flow-list QOS-LIST3**

Creates an IPv4 QoS flow list (`QOS-LIST3`). After creating the list, the command switches to IPv4 QoS flow list mode.

3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-3**

Configures the IPv4 QoS flow list in which the policer entry (`POLICER-3`) is specified for flows whose destination IP address is 192.0.2.10.

4. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

5. **(config)# interface gigabitethernet 1/3.100**

Switches to configuration command mode for Ethernet subinterface 1/3.100.

6. **(config-subif)# ip qos-flow-group QOS-LIST3 in**

Applies the IPv4 QoS flow list (QOS-LIST3) to the receiving side.

#### 4.2.5 Configuring the combined use of maximum bandwidth monitoring and minimum bandwidth monitoring

The following describes an example of performing maximum and minimum bandwidth monitoring for a certain type of flow and updating DSCP for non-compliant frames.

##### Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then maximum and minimum bandwidth monitoring is performed. The DSCP value of any non-compliant frames found during minimum bandwidth monitoring is changed.

##### Command examples

1. **(config)# policer POLICER-4 in max-rate 800M max-burst 120k min-rate 300M min-burst 70k penalty-dscp 22**

Creates a policer entry (POLICER-4) and sets the values as follows:

- Monitoring bandwidth for maximum bandwidth monitoring: 800 Mbit/s
- Burst size for maximum bandwidth monitoring: 120 KB
- Monitoring bandwidth for minimum bandwidth monitoring: 300 Mbit/s
- Burst size for minimum bandwidth monitoring: 70 KB
- DSCP value for non-compliant frames in minimum bandwidth monitoring: 22

2. **(config)# ip qos-flow-list QOS-LIST4**

Creates an IPv4 QoS flow list (QOS-LIST4). After creating the list, the command switches to IPv4 QoS flow list mode.

3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-4**

Configures the IPv4 QoS flow list in which the policer entry (POLICER-4) is specified for flows whose destination IP address is 192.0.2.10.

4. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

5. **(config)# interface port-channel 20.200**

Switches to configuration command mode for port channel subinterface 20.200.

6. **(config-subif)# ip qos-flow-group QOS-LIST4 in**

Applies the IPv4 QoS flow list (QOS-LIST4) to the receiving side.

### 4.2.6 Configuring maximum bandwidth monitoring with an aggregate policer

The following describes an example for bandwidth monitoring for multiple flows by applying a policer entry to multiple QoS flow entries and interfaces.

#### Points to note

A policer entry for maximum bandwidth monitoring is applied to two QoS flow entries that are detected by different TCP port numbers. If you set these QoS flow entries to two interfaces, the bandwidth for four flows is monitored at the same time.

#### Command examples

1. **(config)# policer POLICER-5 in max-rate 800M max-burst 200k**

Creates a policer entry (POLICER-5) and sets the values as follows:

- Monitoring bandwidth for maximum bandwidth monitoring: 800 Mbit/s
- Burst size for maximum bandwidth monitoring: 200 KB

2. **(config)# ip qos-flow-list QOS-LIST5**

Creates an IPv4 QoS flow list (QOS-LIST5). After creating the list, the command switches to IPv4 QoS flow list mode.

3. **(config-ip-qos)# qos tcp any any eq http action policer POLICER-5**

Configures the IPv4 QoS flow list in which a policer entry (POLICER-5) is specified for TCP flows with the destination port number for HTTP.

4. **(config-ip-qos)# qos tcp any any eq ftp action policer POLICER-5**

Configures the IPv4 QoS flow list in which a policer entry (POLICER-5) is specified for TCP flows with the destination port number for FTP.

5. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

6. **(config)# interface gigabitethernet 1/3**

Switches to configuration command mode for Ethernet interface 1/3.

7. **(config-if)# ip qos-flow-group QOS-LIST5 in**

Applies the IPv4 QoS flow list (QOS-LIST5) to the receiving side.

8. **(config-if)# exit**

Changes the mode from the configuration command mode for Ethernet interface 1/3 to global configuration mode.



9. **(config)# interface gigabitethernet 1/4**  
Switches to configuration command mode for Ethernet interface 1/4.
10. **(config-if)# ip qos-flow-group QOS-LIST5 in**  
Applies the IPv4 QoS flow list (QOS-LIST5) to the receiving side.

## 4.3 Operation

### 4.3.1 List of operation commands

The following table describes the operation commands for the policer.

*Table 4-5: List of operation commands*

Command name	Description
show qos-flow	Shows QoS flow setting details and statistics.
show policer	Shows policer setting details and statistics.
clear policer	Clears the policer statistics.

### 4.3.2 Checking the details of maximum bandwidth monitoring

You can use the `show qos-flow` command and the `show policer` command to check the details of maximum bandwidth monitoring. Execute the `show qos-flow` command and confirm that the message `refer to policer statistics` is displayed in the QoS flow statistics. Next, execute the `show policer` command to check the policer statistics.

*Figure 4-3: Result of executing the show qos-flow command*

```
> show qos-flow interface gigabitethernet 1/1 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 in
IP qos-flow-list : QOS-LIST1
    10 ip any host 192.0.2.10 action policer POLICER-1
        refer to policer statistics
```

Confirm that the policer entry (POLICER-1) and the message `refer to policer statistics` are displayed in the listed information of QOS-LIST1.

*Figure 4-4: Result of executing the show policer command*

```
> show policer POLICER-1
Date 20XX/01/01 12:00:00 UTC
policer POLICER-1 in
    max-rate 500M max-burst 100k
        Total                Matched packets
        Max-rate over   :           146723
        Max-rate under  :          2118673486
    PRU 1                  Matched packets
        Max-rate over   :           146723
        Max-rate under  :          2118673486
```

Confirm that the following items are included in the information for POLICER-1:

- Monitoring bandwidth for maximum bandwidth monitoring: `max-rate 500M`
- Burst size for maximum bandwidth monitoring: `max-burst 100k`

You can check non-compliant frames by checking the value of `Matched packets` for `Max-rate over`. You can check compliant frames by checking the value of `Matched packets` for `Max-rate under`.

### 4.3.3 Checking discard class for non-compliant minimum bandwidth monitoring

You can use the `show qos-flow` command and the `show policer` command to check the discard class for non-compliant minimum bandwidth monitoring. Execute the `show qos-flow` command

and confirm that the message refer to policer statistics is displayed in the QoS flow statistics. Next, execute the `show policer` command to check the policer statistics.

*Figure 4-5: Result of executing the show qos-flow command*

```
> show qos-flow interface gigabitethernet 1/3 out
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/3 out
IP qos-flow-list : QOS-LIST2
    10 ip any host 192.0.2.10 action policer POLICER-2
        refer to policer statistics
```

Confirm that the policer entry (POLICER-2) and the message refer to policer statistics are displayed in the listed information of QOS-LIST2.

*Figure 4-6: Result of executing the show policer command*

```
> show policer POLICER-2
Date 20XX/01/01 12:00:00 UTC
policer POLICER-2 out
    min-rate 300M min-burst 80k penalty-discard-class 2
      Total
        Min-rate over   : 146723
        Min-rate under  : 2118673486
      PRU 1
        Min-rate over   : 146723
        Min-rate under  : 2118673486
```

Confirm that the following items are included in the information for POLICER-2:

- Monitoring bandwidth for minimum bandwidth monitoring: min-rate 300M
- Burst size for minimum bandwidth monitoring: min-burst 80k
- Discard class for non-compliant frames: penalty-discard-class 2

You can check non-compliant frames by checking the value of Matched packets for Min-rate over. You can check compliant frames by checking the value of Matched packets for Min-rate under.

#### 4.3.4 Checking DSCP rewrite when non-compliance occurs in minimum monitoring bandwidth

You can use the `show qos-flow` command and the `show policer` command to check DSCP rewrite for non-compliant minimum bandwidth monitoring. Execute the `show qos-flow` command and confirm that the message refer to policer statistics is displayed in the QoS flow statistics. Next, execute the `show policer` command to check the policer statistics.

*Figure 4-7: Result of executing the show qos-flow command*

```
> show qos-flow interface gigabitethernet 1/3.100 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/3.100 in
IP qos-flow-list : QOS-LIST3
    10 ip any host 192.0.2.10 action policer POLICER-3
        refer to policer statistics
```

Confirm that the policer entry (POLICER-3) and the message refer to policer statistics are displayed in the listed information of QOS-LIST3.

*Figure 4-8: Result of executing the show policer command*

```
> show policer POLICER-3
Date 20XX/01/01 12:00:00 UTC
policer POLICER-3 in
    min-rate 200M min-burst 70k penalty-dscp 11
      Total
        Matched packets
```

```

Min-rate over : 146723
Min-rate under : 2118673486
PRU 1 Matched packets
Min-rate over : 146723
Min-rate under : 2118673486

```

Confirm that the following items are included in the information for POLICER-3:

- Monitoring bandwidth for minimum bandwidth monitoring: min-rate 200M
- Burst size for minimum bandwidth monitoring: min-burst 70k
- DSCP value for non-compliant frame: penalty-dscp 11

You can check non-compliant frames by checking the value of Matched packets for Min-rate over. You can check compliant frames by checking the value of Matched packets for Min-rate under.

### 4.3.5 Checking the combined use of maximum bandwidth monitoring and minimum bandwidth monitoring

You can use the `show qos-flow` command and the `show policer` command to check the details on combined use of maximum bandwidth monitoring and minimum bandwidth monitoring. Execute the `show qos-flow` command and confirm that the message refer to policer statistics is displayed in the QoS flow statistics. Next, execute the `show policer` command to check the policer statistics.

*Figure 4-9: Result of executing the show qos-flow command*

```

> show qos-flow interface port-channel 20.200 in
Date 20XX/01/01 12:00:00 UTC
Using interface : port-channel 20.200 in
IP qos-flow-list : QOS-LIST4
    10 ip any host 192.0.2.10 action policer POLICER-4
        refer to policer statistics

```

Confirm that the policer entry (POLICER-4) and the message refer to policer statistics are displayed in the listed information of QOS-LIST4.

*Figure 4-10: Result of executing the show policer command*

```

> show policer POLICER-4
Date 20XX/01/01 12:00:00 UTC
policer POLICER-4 in
    max-rate 800M max-burst 120k min-rate 300M min-burst 70k penalty-dscp af23(22)
    Total Matched packets
        Max-rate over : 502491
        Min-rate over : 64729081
        Min-rate under : 2883808952
    PRU 1 Matched packets
        Max-rate over : 26834
        Min-rate over : 146723
        Min-rate under : 2118673486
    PRU 3 Matched packets
        Max-rate over : 475657
        Min-rate over : 64582358
        Min-rate under : 765135484

```

Confirm that the following items are included in the information for POLICER-4:

- Monitoring bandwidth for maximum bandwidth monitoring: max-rate 800M
- Burst size for maximum bandwidth monitoring: max-burst 120k
- Monitoring bandwidth for minimum bandwidth monitoring: min-rate 300M

- Burst size for minimum bandwidth monitoring: min-burst 70k
- DSCP value for non-compliant frame: penalty-dscp 22

You can check non-compliant frames in maximum bandwidth monitoring by checking the value of `Matched packets for Max-rate over`. Also, you can check non-compliant frames in minimum bandwidth monitoring by checking the value of `Matched packets for Min-rate over`. You can check compliant frames in minimum bandwidth monitoring by checking the value of `Matched packets for Min-rate under`.

### 4.3.6 Checking the details of maximum bandwidth monitoring with an aggregate policer

You can use the `show qos-flow` command and the `show policer` command to check the details of maximum bandwidth monitoring with aggregate policer. Execute the `show qos-flow` command and confirm that the message `refer to policer statistics` is displayed in the QoS flow statistics. Next, execute the `show policer` command to check the policer statistics.

*Figure 4-11: Result of executing the show qos-flow command*

```
> show qos-flow interface gigabitethernet 1/3 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/3 in
IP qos-flow-list : QOS-LIST5
    10 tcp(6) any any eq http(80) action policer POLICER-5
        refer to policer statistics
    20 tcp(6) any any eq ftp(21) action policer POLICER-5
        refer to policer statistics

> show qos-flow interface gigabitethernet 1/4 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/4 in
IP qos-flow-list : QOS-LIST5
    10 tcp(6) any any eq http(80) action policer POLICER-5
        refer to policer statistics
    20 tcp(6) any any eq ftp(21) action policer POLICER-5
        refer to policer statistics
```

Confirm that the policer entry (POLICER-5) and the message `refer to policer statistics` are displayed in the listed information of QOS-LIST5.

*Figure 4-12: Result of executing the show policer command*

```
> show policer POLICER-5
Date 20XX/01/01 12:00:00 UTC
policer POLICER-5 in
    max-rate 800M max-burst 200k
    Total                               Matched packets
        Max-rate over :                   2745392
        Max-rate under :                  125343477
    PRU 1                               Matched packets
        Max-rate over :                   2745392
        Max-rate under :                  125343477
```

Confirm that the following items are included in the information for POLICER-5:

- Monitoring bandwidth for maximum bandwidth monitoring: max-rate 800M
- Burst size for maximum bandwidth monitoring: max-burst 200k

In the multiple flows for which the policer entry (POLICER-5) is specified, you can check non-compliant frames by checking the value of `Matched packets for Max-rate over`. You can check compliant frames by checking the value of `Matched packets for Max-rate under`.



## Chapter

---

# 5. Marker

---

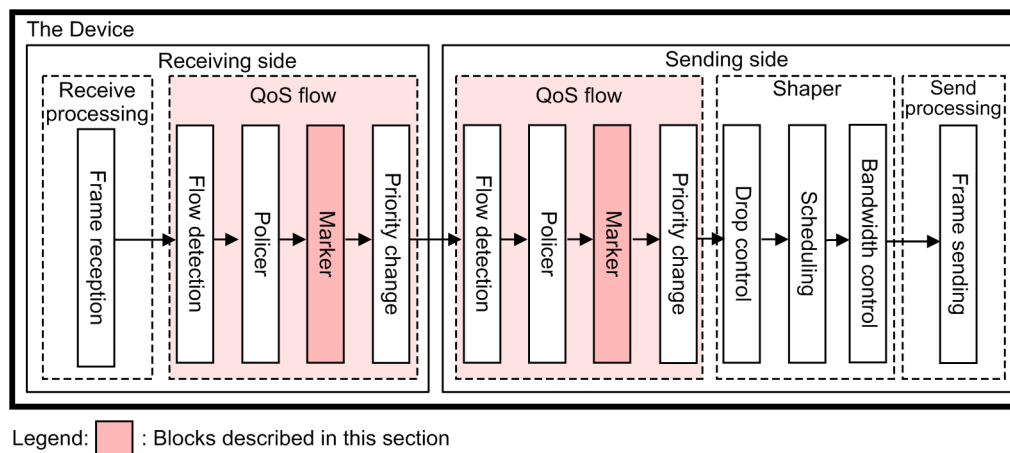
The marker functionality is used to update the user priority and the DSCP for frames detected by QoS flow detection. This chapter describes the marker and how to use it.

- 5.1 Description
- 5.2 Configuration
- 5.3 Operation

## 5.1 Description

The marker functionality is used to update the user priority in a VLAN tag and the DSCP value in an IP header for frames detected by flow detection. The following figure shows the positioning of the marker block described in this section.

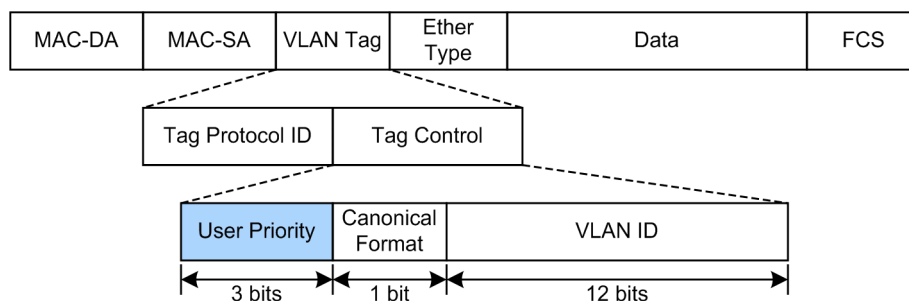
Figure 5-1: Positioning of the marker block



### 5.1.1 User priority rewrite

User priority rewrite is functionality that updates the user priority in the VLAN tag of a frame detected by flow detection. The user priority is the three highest-order bits of the Tag Control field shown in the following figure:

Figure 5-2: Header format of a VLAN tag



If the user priority rewrite functionality is used, the user priority of the packet is rewritten when the Device forwards an IP packet. The user priority becomes 0 if the user priority rewrite is not used.

### 5.1.2 DSCP rewrite

DSCP rewrite is functionality that is used to update the DSCP, which is the six highest-order bits of the TOS field in the IPv4 header or the traffic class field in the IPv6 header. The following figures show the formats of the TOS and traffic class fields.



Figure 5-3: Format of the TOS field

Format of the IPv4 header

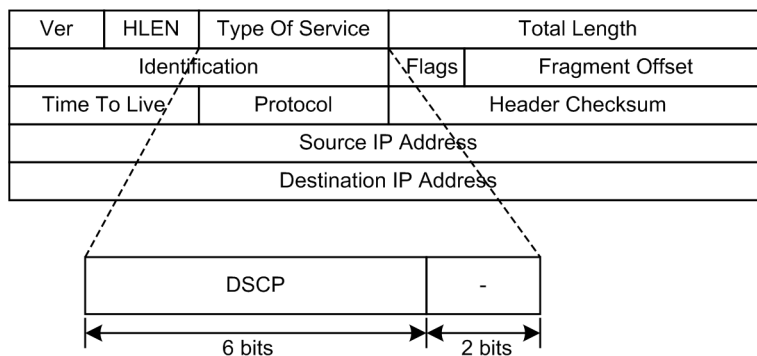
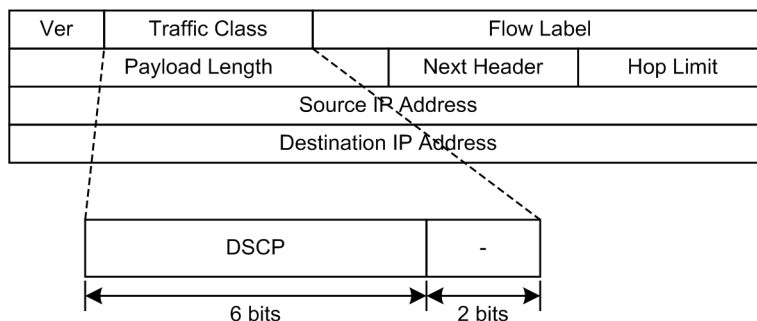


Figure 5-4: Format of the traffic class field

Format of the IPv6 header



### 5.1.3 Notes on using the marker

#### (1) Operation when markers are specified for the receiving interface and sending interface

If flow detection is set up with markers for the receiving and sending interfaces and frames are matched at both interfaces, the frames are sent with the marker applied at the sending interface.

## 5.2 Configuration

### 5.2.1 List of configuration commands

The following table describes the configuration commands for the marker.

*Table 5-1:* List of configuration commands

Command name	Description
advance qos-flow-group	Sets an Advance QoS flow list to an interface and applies QoS control based on Advance conditions.
advance qos-flow-list	Sets the Advance QoS flow list that is used for the flow detection based on Advance conditions.
advance qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the Advance QoS flow list are applied.
ip qos-flow-group	Applies an IPv4 QoS flow list to an interface and enables IPv4 QoS control.
ip qos-flow-list	Sets the QoS flow list used for IPv4 QoS flow detection.
ip qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv4 QoS flow list are applied.
ipv6 qos-flow-group	Applies an IPv6 QoS flow list to an interface and enables IPv6 QoS control.
ipv6 qos-flow-list	Sets the QoS flow list used for IPv6 QoS flow detection.
ipv6 qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv6 QoS flow list are applied.
mac qos-flow-group	Applies a MAC QoS flow list to an interface and enables MAC QoS control.
mac qos-flow-list	Sets the QoS flow list used for MAC QoS flow detection.
mac qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the MAC QoS flow list are applied.
qos	Specifies flow detection conditions and action specifications in the QoS flow list.

### 5.2.2 Configuring user priority rewrite

The following example shows how to rewrite the user priority for a certain type of flow.

#### Points to note

When frames are sent, first flow detection is performed based on the destination IP address, and then the user priority is rewritten.

#### Command examples

1. **(config)# ip qos-flow-list QOS-LIST1**

Creates an IPv4 QoS flow list (QOS-LIST1). After creating the list, the command switches to IPv4 QoS flow list mode.

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action replace-user-priority 6**

Configures the IPv4 QoS flow list in which the user priority is rewritten to 6 for flows whose destination IP address is 192.0.2.10.

3. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

4. **(config)# interface gigabitethernet 1/2.30**

Switches to configuration command mode for Ethernet subinterface 1/2.30.

5. **(config-subif)# ip qos-flow-group QOS-LIST1 out**

Applies the IPv4 QoS flow list (QOS-LIST1) on the sending side.

### 5.2.3 Configuring DSCP rewrite

The following describes an example of updating the DSCP for a certain type of flow.

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then the DSCP value is updated.

Command examples

1. **(config)# ip qos-flow-list QOS-LIST2**

Creates an IPv4 QoS flow list (QOS-LIST2). After creating the list, the command switches to IPv4 QoS flow list mode.

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action replace-dscp 63**

Configures the IPv4 QoS flow list in which the DSCP value is updated to 63 for flows whose destination IP address is 192.0.2.10.

3. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

4. **(config)# interface port-channel 10.30**

Switches to configuration command mode for port channel subinterface 10.30.

5. **(config-subif)# ip qos-flow-group QOS-LIST2 in**

Applies the IPv4 QoS flow list (QOS-LIST2) on the receiving side.

## 5.3 Operation

### 5.3.1 List of operation commands

The following table describes the operation commands for the marker.

*Table 5-2: List of operation commands*

Command name	Description
show qos-flow	Shows QoS flow setting details and statistics.
clear qos-flow	Clears the QoS flow statistics.

### 5.3.2 Checking user priority rewrite

The following figure shows how to check user priority rewrite.

*Figure 5-5: Checking user priority rewrite*

```
> show qos-flow interface gigabitethernet 1/2.30 QOS-LIST1 out
Date 20XX/01/01 12:00:00 UTC
Using interface: gigabitethernet 1/2.30 out
IP qos-flow-list:QOS-LIST1
  10 ip any host 192.0.2.10 action replace-user-priority 6
      Matched packets      Matched bytes
Total   :                74699826      100097766840
PRU 1   :                74699826      100097766840
```

Make sure that `replace-user-priority 6` is displayed in the information for `QOS-LIST1`. You can check the frames that match the flow detection condition by checking the value of `Matched packets` for `Matched bytes`.

### 5.3.3 Checking DSCP rewrite

The following figure shows how to check the DSCP rewrite.

*Figure 5-6: Checking DSCP rewrite*

```
> show qos-flow interface port-channel 10.30 QOS-LIST2 in
Date 20XX/01/01 12:00:00 UTC
Using interface: port-channel 10.30 in
IP qos-flow-list:QOS-LIST2
  10 ip any host 192.0.2.10 action replace-dscp 63
      Matched packets      Matched bytes
Total   :                83436032      111804282880
PRU 1   :                74699826      100097766840
PRU 2   :                8736206       11706516040
```

Make sure that `replace-dscp 63` is displayed in the information for `QOS-LIST2`. You can check the frames that match the flow detection condition by checking the value of `Matched packets` for `Matched bytes`.

## Chapter

---

# 6. Priority Change

---

The priority change functionality is used to change the priority class and discard class for the frames detected by QoS flow detection. This chapter describes priority change and how to use it.

- 6.1 Description
- 6.2 Configuration
- 6.3 Operation

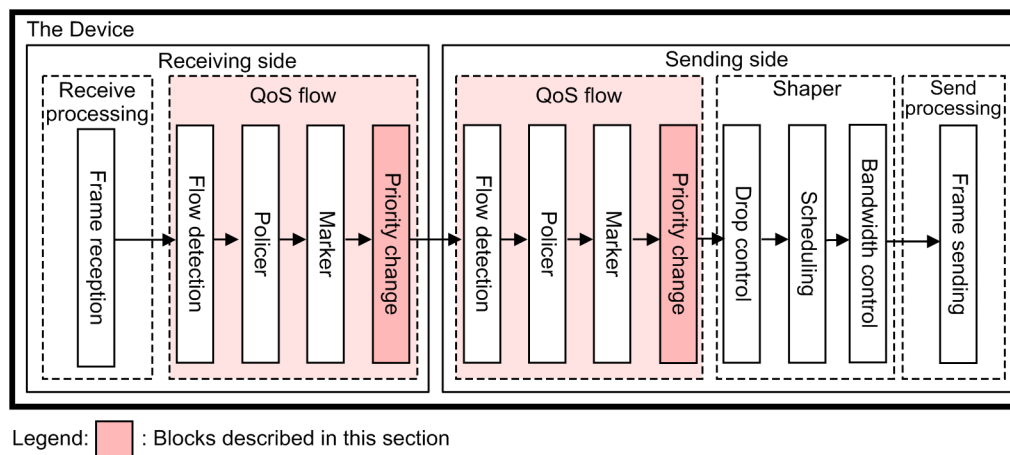
## 6.1 Description

The priority change functionality is used to change the priority class and discard class for the frames detected by flow detection. The following two methods are available for priority change:

- Direct specification of priority class and discard class
- DSCP mapping

The following figure shows the positioning of the priority change block described in this section.

Figure 6-1: Positioning of the priority change block



### 6.1.1 Direct specification of priority class and discard class

This functionality is used to directly specify the priority class and discard class for a detected flow. The priority class indicates whether a frame is to be queued in a queue. The discard class indicates how easily a frame can be discarded when being queued. The following table describes the specifiable range of priority class and discard class.

Table 6-1: Specifiable range of priority class and discard class

Item	Range
Priority class	1 to 8
Discard class	1 to 4

For details about the relationships between the priority class and queue mapping, and relationships between discard class and queuing priority, see 7.1 Description.

### 6.1.2 DSCP mapping

The DSCP mapping functionality is used to determine fixed priority class and discard class for frames based on the DSCP value. The DSCP value substitutes the six highest-order bits of the TOS field or traffic class field.

The following table describes the priority class and discard class values corresponding to DSCP values.

Table 6-2: Priority class and discard class values corresponding to DSCP values

DSCP value	Priority class	Discard class
0 to 7	1	4

DSCP value	Priority class	Discard class
8 to 9	2	1
10 to 11		4
12 to 13		3
14 to 15		2
16 to 17	3	1
18 to 19		4
20 to 21		3
22 to 23		2
24 to 25	4	1
26 to 27		4
28 to 29		3
30 to 31		2
32 to 33	5	1
34 to 35		4
36 to 37		3
38 to 39		2
40 to 47	6	1
48 to 55	7	1
56 to 63	8	1

### 6.1.3 Notes on using priority change

#### (1) *Priority of operations in priority change*

The priority class and discard class are determined by direct specification or DSCP mapping. The priority order for priority changes is described below. A smaller number represents a higher priority.

1. DSCP mapping set at the sending interface
2. Direct specification of priority class and discard class set at the sending interface
3. DSCP mapping set at the receiving interface
4. Direct specification of priority class and discard class set at the receiving interface

#### (2) *Using direct specification and DSCP mapping together*

You cannot use direct specification of priority class and DSCP mapping at the same time for a single QoS flow entry.

#### (3) *Operation when using DSCP rewrite and DSCP mapping together*

Priority class and discard class are changed according to the updated DSCP value if DSCP rewrite and DSCP mapping are used together for a single flow.

## 6.2 Configuration

### 6.2.1 List of configuration commands

The following table describes the configuration commands for priority change.

*Table 6-3:* List of configuration commands

Command name	Description
advance qos-flow-group	Sets an Advance QoS flow list to an interface and applies QoS control based on Advance conditions.
advance qos-flow-list	Sets the Advance QoS flow list that is used for the flow detection based on Advance conditions.
advance qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the Advance QoS flow list are applied.
ip qos-flow-group	Applies an IPv4 QoS flow list to an interface and enables IPv4 QoS control.
ip qos-flow-list	Sets the QoS flow list used for IPv4 QoS flow detection.
ip qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv4 QoS flow list are applied.
ipv6 qos-flow-group	Applies an IPv6 QoS flow list to an interface and enables IPv6 QoS control.
ipv6 qos-flow-list	Sets the QoS flow list used for IPv6 QoS flow detection.
ipv6 qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv6 QoS flow list are applied.
mac qos-flow-group	Applies a MAC QoS flow list to an interface and enables MAC QoS control.
mac qos-flow-list	Sets the QoS flow list used for MAC QoS flow detection.
mac qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the MAC QoS flow list are applied.
qos	Specifies flow detection conditions and action specifications in the QoS flow list.
remark	Specifies supplementary information for QoS.

### 6.2.2 Configuring a priority class change

The following example shows how to change the priority class for a certain type of flow.

#### Points to note

When frames are sent, first flow detection is performed based on the destination IP address, and then priority change is performed.

#### Command examples

1. **(config)# ip qos-flow-list QOS-LIST1**

Creates an IPv4 QoS flow list (QOS-LIST1). After creating the list, the command switches to IPv4 QoS flow list mode.

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action**



**priority-class 6**

Configures the IPv4 QoS flow list in which the priority class is rewritten to 6 for flows whose destination IP address is 192.0.2.10.

3. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

4. **(config)# interface gigabitethernet 1/3**

Switches to configuration command mode for Ethernet interface 1/3.

5. **(config-if)# ip qos-flow-group QOS-LIST1 out**

Applies the IPv4 QoS flow list (QOS-LIST1) on the sending side.

### 6.2.3 Configuring DSCP mapping

The following example shows how to use DSCP mapping to change priority class and discard class for a certain type of flow.

#### Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then the priority class and discard class are changed by DSCP mapping.

#### Command examples

1. **(config)# ip qos-flow-list QOS-LIST2**

Creates an IPv4 QoS flow list (QOS-LIST2). After creating the list, the command switches to IPv4 QoS flow list mode.

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action dscp-map**

Configures the IPv4 QoS flow list for destination IP address 192.0.2.10, and changes the priority class and discard class by DSCP mapping.

3. **(config-ip-qos)# exit**

Returns to global configuration mode from IPv4 QoS flow list mode.

4. **(config)# interface gigabitethernet 1/3.50**

Switches to configuration command mode for Ethernet subinterface 1/3.50.

5. **(config-subif)# ip qos-flow-group QOS-LIST2 in**

Applies the IPv4 QoS flow list (QOS-LIST2) on the receiving side.

## 6.3 Operation

### 6.3.1 List of operation commands

The following table describes the operation commands for priority change.

*Table 6-4:* List of operation commands

Command name	Description
show qos-flow	Shows QoS flow setting details and statistics.
clear qos-flow	Clears the QoS flow statistics.

### 6.3.2 Checking priority change

You can use the `show qos queueing port` command to check the details of the priority change. You can check the change in the priority class by the queue number of the queued frames. The following figure shows the result of executing the command.

*Figure 6-2:* Checking priority change

```
> show qos queueing port 1/3 out
Date 20XX/01/01 12:00:00 UTC
NIF1/Port3 (Out)
Max-queue=8
Queue1 : Qlen=0, Peak-Qlen=0, Limit-Qlen=1023
        Drop-mode=tail-drop
        Discard      Send packet      Discard packet      Send byte
        1            0                0                  -
        2            0                0                  -
        3            0                0                  -
        4            0                0                  -
        Total        0                0                  0
        :
Queue6 : Qlen=0, Peak-Qlen=51, Limit-Qlen=1023
        Drop-mode=tail-drop
        Discard      Send packet      Discard packet      Send byte
        1            3203665          0                  -
        2            0                0                  -
        3            0                0                  -
        4            0                0                  -
        Total        3203665          0                  4850293146
        :
Queue8 : Qlen=0, Peak-Qlen=0, Limit-Qlen=1023
        Drop-mode=tail-drop
        Discard      Send packet      Discard packet      Send byte
        1            0                0                  -
        2            0                0                  -
        3            0                0                  -
        4            0                0                  -
        Total        0                0                  0
>
```

Make sure that the value for `Queue6` has a count value.

## Chapter

---

# 7. Port Shaper

---

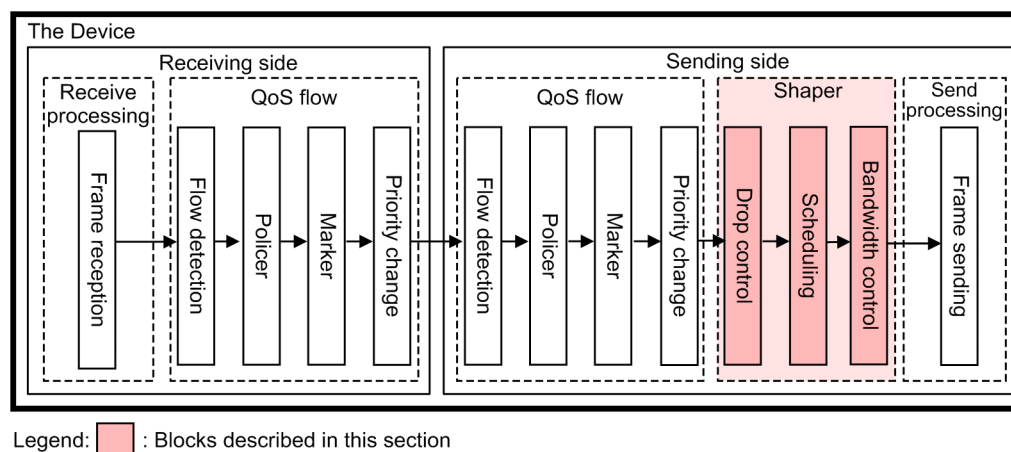
The port shaper functionality is used to control the priority order for queuing, output order of frames from queues, and output bandwidth for ports. This chapter describes the port shaper and how to use it.

- 7.1 Description
- 7.2 Configuration
- 7.3 Operation
- 7.4 Correspondence between NIFs and port shapers

## 7.1 Description

The shaper functionality is used to control the priority order when queuing, the output order of frames from each queue, and the output bandwidth for each port. The following figure shows the positioning of the shaper block described in this section.

Figure 7-1: Positioning of the shaper block

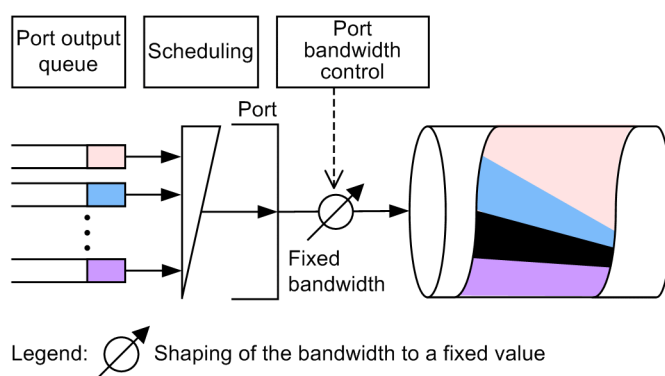


### 7.1.1 Overview

The port shaper functionality operates in port output queues. A port shaper consists of drop control that determines whether to queue or discard the frames, scheduling that determines the queue from which the next frame will be sent, and port bandwidth control that shapes the Ethernet interface bandwidth.

The following figure shows an overview of the port shaper.

Figure 7-2: Overview of the port shaper (mounted in port output queues)



### 7.1.2 Drop control

The drop control functionality controls the queuing priority, which indicates how easily a frame can be dropped from a queue, and controls whether the frame can be queued or dropped according to the number of retained frames. Queuing priority is mapped by the discard class determined by flow control or policer. If frames remain in a queue, you can implement more detailed QoS by changing the queuing priority. The Device uses the tail drop method for drop control.

#### (1) Discard class and mapping queuing priority

Queuing priority is mapped by the discard class determined by flow control or policer. The following table describes the relationship between a discard class and queuing priority.

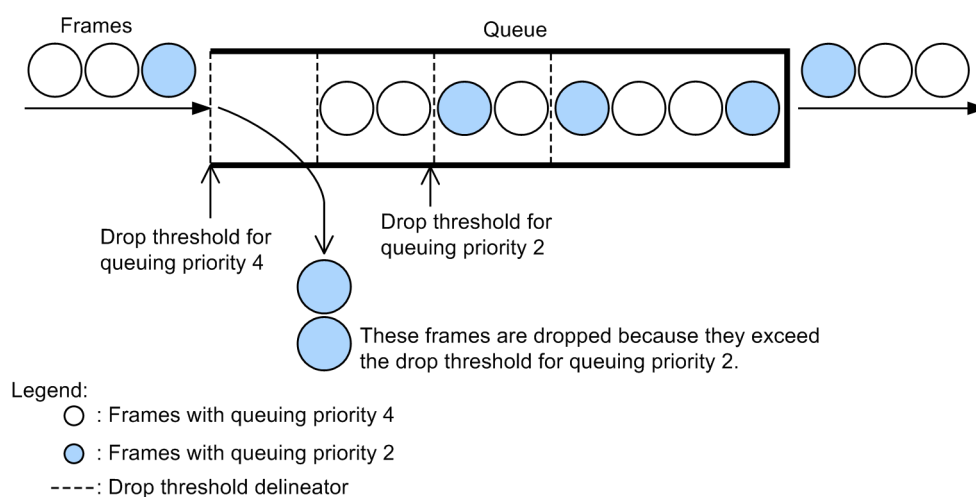
Table 7-1: Relationship between a discard class and queuing priority

Discard class	Queuing priority
1	1
2	2
3	3
4	4

## (2) Tail drop

The tail drop method functionality drops frames if the queue length exceeds the drop threshold. The drop threshold varies depending on the queuing priority. Frames in a queue that has a higher queuing priority are more difficult to drop. The following figure shows an overview of the tail drop method. When the drop threshold for queuing priority 2 is exceeded, the queuing priority 2 frames are all dropped.

Figure 7-3: Overview of the tail drop method



The following table describes the queuing priorities and corresponding drop thresholds for the tail drop method. The drop threshold indicates the percentage of frames remaining in the queue to the queue length.

Table 7-2: Queuing priorities and corresponding drop thresholds

Queuing priority	Drop threshold (%)
1	40
2	60
3	85
4	100

## 7.1.3 Scheduling

Scheduling is functionality that controls the order in which the frames in each queue will be sent. The Device provides the scheduling types below. The following table describes the scheduling operations:

Table 7-3: Scheduling operations

Scheduling type	Conceptual diagram	Operation	Application example
PQ		Complete priority queuing. When there are frames in multiple queues, the frames in a higher-priority queue are always sent first.	When traffic priority must be strictly observed
RR		Round robin. If there are frames in multiple queues, the queues are checked in order and then the frames are sent out one by one. Queues are controlled so that they have an equal number of frames regardless of the frame length.	When all traffic must be equal in terms of the number of frames
4PQ+4WFQ		Control by using four top-priority queues + four weighted fair queues. Frames in queues 8, 7, 6, and 5 (Q#8, Q#7, Q#6, and Q#5 in the figure on the left) are subject to complete priority queuing. If there are no frames in queues 8 through 5, the frames in queues 4, 3, 2, and 1 (Q#4, Q#3, Q#2, and Q#1 in the figure on the left) are sent according to a predetermined bandwidth ratio ( $w:x:y:z$ ).	When PQ queues carry traffic whose priority order must be strictly observed. When WFQ queues carry traffic that uses surplus bandwidth of PQ in the predetermined bandwidth ratio.
2PQ+4WFQ+2BEQ		Control by using two top-priority queues + four weighted fair queues + two best-effort queues. Frames in queues 8, and 7 (Q#8 and Q#7 in the figure on the left) are subject to complete priority queuing. If there are no frames in queues 8 and 7, the frames in queues 6, 5, 4, and 3 (Q#6, Q#5, Q#4, and Q#3 in the figure on the left) are sent according to a predetermined bandwidth ratio ( $w:x:y:z$ ). If there are no frames in queues 8 through 3, frames in queues 2 and 1 (Q#2 and Q#1 in the figure on the left) are subject to complete priority queuing.	When PQ queues carry traffic whose priority order must be strictly observed. When WFQ queues carry traffic that uses surplus bandwidth of PQ in the predetermined bandwidth ratio. When BEQ queues carry traffic that uses surplus bandwidth of PQ or WFQ.

Scheduling type	Conceptual diagram	Operation	Application example
4WFQ+4BEQ		Control by using four weighted fair queues + four best-effort queues. Frames in queues 8, 7, 6, and 5 (Q#8, Q#7, Q#6, and Q#5 in the figure on the left) are sent according to a predetermined bandwidth ratio ( $w:x:y:z$ ). If there are no frames in queues 8 through 5, frames in queues 4, 3, 2 and 1 (Q#4, Q#3, Q#2, and Q#1 in the figure on the left) are subject to complete priority control.	When WFQ queues carry traffic with the predetermined ratio. When BEQ queues carry traffic that uses surplus bandwidth of WFQ.

Table 7-4: Scheduling specifications

Item		Specific ations	Description
Number of queues	PQ RR	1, 2, 4, or 8 queues	You can specify 1, 2, 4, or 8 queues. By changing the number of queues, you can increase the queue length.
	4PQ+4WFQ 2PQ+4WFQ+2BEQ 4WFQ+4BEQ	8 queues	Fixed to 8 queues.
4WFQ weightin g	4PQ+4WFQ 2PQ+4WFQ+2BEQ 4WFQ+4BEQ	1% to 97%	Make sure that the bandwidth ratio ( $w:x:y:z$ ) used for weighting under 4WFQ satisfies the following conditions: $w \geq x \geq y \geq z$ and $w + x + y + z = 100$

The selectable scheduling type depends on NIF. For details about the corresponding NIF, see *7.4 Correspondence between NIFs and port shapers*. Note that the default scheduling type is set to PQ.

### 7.1.4 Queue number specification

The queue number specification functionality changes the number of port output queues. The default value is set to 8 queues.

The queue length per queue is increased if you change the number of queues from eight to four, two, or one. Queue length represents the number of packet buffers that can be used in a queue.

#### (1) Relationship between the number of queues and queue length

The allowed queue length varies according to the number of queues for each port and the NIF in use. The following table describes queue length per queue according to the number of queues per port and the NIF to be used.

Table 7-5: Queue length per queue

Abbreviated name of NIF model	Number of queues per port			
	8 queues	4 queues	2 queues	1 queue
NL1G-12T	511	1023	2047	4095
NL1G-12S	511	1023	2047	4095
NLXG-6RS	1023	2047	4095	8191
NMCG-1C	4095	8191	16383	32767

## (2) Priority class and queue number mapping

The queue number for queued frame is mapped according to the priority class determined by the flow control. Also, the queue number for queued frames differs depending on the number of queues. The following table describes the relationship between the priority class and the queue number for queued frames.

Table 7-6: Relationship between the priority class and the queue number for queued frame

Priority class	Queue number for queued frame by number of queues			
	8 queues	4 queues	2 queues	1 queue
1	1	1	1	1
2	2			
3	3			
4	4	2	2	
5	5			
6	6			
7	7	3	2	
8	8			

### 7.1.5 Port bandwidth control

The port bandwidth control functionality shapes the traffic to the send bandwidth specified for the relevant port after scheduling is performed. You can use this control to connect to services such as wide-area Ethernet services.

For example, if the port bandwidth is 1 Gbit/s and the contract bandwidth with the ISP is 400 Mbit/s, you can use port bandwidth control functionality to suppress the bandwidth to 400 Mbit/s or less when sending frames.

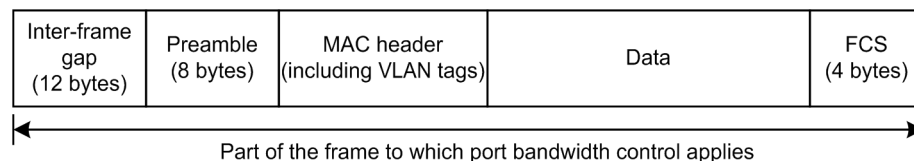
The following table describes the specification of port bandwidth control.

Table 7-7: Specification of port bandwidth control

Setting unit	Setting range	Increment
Gbit/s	1 to 100 Gbit/s	1 Gbit/s
Mbit/s	1 to 100000 Mbit/s	1 Mbit/s
kbit/s	10 to 100000000 kbit/s	10 kbit/s

The part of a frame to which port bandwidth control applies is from the inter-frame gap to FCS. The following figure shows the part of the frame to which port bandwidth control applies.

Figure 7-4: Part of the frame to which port bandwidth control applies





## 7.1.6 Notes on using the port shaper

### **(1) Notes on queue number specification**

If you change the current number of queues to a different number of queues by using queue number specification, the frames remaining in the queues before the change are discarded.

### **(2) Notes on using port bandwidth control in half duplex mode**

If you use the port bandwidth control in the following interfaces, the send bandwidth cannot be set to the bandwidth specified by port bandwidth control:

- Ethernet interface with half duplex mode
- Ethernet interface turning into half duplex mode as a result of auto-negotiation

## 7.2 Configuration

### 7.2.1 List of configuration commands

The following table describes the configuration commands for port shaper.

*Table 7-8:* List of configuration commands

Command name	Description
advance qos-flow-group	Sets an Advance QoS flow list to an interface and applies QoS control based on Advance conditions.
advance qos-flow-list	Sets the Advance QoS flow list that is used for the flow detection based on Advance conditions.
ip qos-flow-group	Applies an IPv4 QoS flow list to an interface and enables IPv4 QoS control.
ip qos-flow-list	Sets the QoS flow list used for IPv4 QoS flow detection.
ipv6 qos-flow-group	Applies an IPv6 QoS flow list to an interface and enables IPv6 QoS control.
ipv6 qos-flow-list	Sets the QoS flow list used for IPv6 QoS flow detection.
mac qos-flow-group	Applies a MAC QoS flow list to an interface and enables MAC QoS control.
mac qos-flow-list	Sets the QoS flow list used for MAC QoS flow detection.
qos	Specifies flow detection conditions and action specifications in the QoS flow list.
qos-queue-group	Applies a QoS queue list to an Ethernet interface and enables the shaper.
qos-queue-list	Sets the scheduling and queue number specification to the QoS queue list that stores the port shaper settings.
traffic-shape rate	Sets port bandwidth control for port shaper to an Ethernet interface.

### 7.2.2 Configuring scheduling

Points to note

A QoS queue list that includes scheduling is created, and then the created list is applied to the sending side of the target Ethernet interface.

Command examples

1. **(config)# qos-queue-list QLIST-PQ pq**  
Sets scheduling (pq) in the QoS queue list (QLIST-PQ).
2. **(config)# interface gigabitethernet 1/1**  
**(config-if)# qos-queue-group QLIST-PQ out**  
Switches to configuration command mode for Ethernet interface 1/1 and applies the QoS queue list (QLIST-PQ) to the sending side.

### 7.2.3 Configuring queue number specification

Points to note

A QoS queue list that includes a queue number specification is created, and then the created list is applied to the sending side of the target Ethernet interface. The types of scheduling to which a queue number specification is applied are PQ (complete priority queuing) and RR

(round robin).

#### Command examples

1. **(config)# qos-queue-list QLIST-PQ-QNUM4 pq number\_of\_queue\_4**  
Sets `pq` as scheduling type and 4 as number of queues in the QoS queue list (QLIST-PQ-QNUM4).
2. **(config)# interface gigabitethernet 1/11**  
**(config-if)# qos-queue-group QLIST-PQ-QNUM4 out**  
Switches to configuration command mode for Ethernet interface 1/11 and applies the QoS queue list (QLIST-PQ-QNUM4) to the sending side.

### 7.2.4 Configuring port bandwidth control

The following describes how to set the output bandwidth of the target Ethernet interface so that it is lower than the bandwidth of the actual line.

#### Points to note

A bandwidth (20 Mbit/s in the example) is set to the target Ethernet interface by using port bandwidth control.

#### Command examples

1. **(config)# interface gigabitethernet 1/12**  
**(config-if)# traffic-shape rate 20M**  
Switches to configuration command mode for Ethernet interface 1/12 and sets the port bandwidth to 20 Mbit/s.

### 7.2.5 Configuring queuing priority

The following describes an example of changing the discard class and setting the queuing priority for a certain type of QoS flow.

#### Points to note

When frames are received, first QoS flow detection is performed based on the destination IP address, and then discard class is changed. Queuing priority is based on discard class.

#### Command examples

1. **(config)# ip qos-flow-list QOS-LIST2**  
Creates an IPv4 QoS flow list (QOS-LIST2). After creating the list, the command switches to IPv4 QoS flow list mode.
2. **(config-ip-qos)# qos ip any host 192.0.2.10 action**  
**priority-class 8 discard-class 1**  
Configures the IPv4 QoS flow list for destination IP address 192.0.2.10, priority class 8, and discard class 1.
3. **(config-ip-qos)# exit**  
Returns to global configuration mode from IPv4 QoS flow list mode.
4. **(config)# interface gigabitethernet 1/3**

```
(config-if)# ip qos-flow-group QOS-LIST2 in
```

Switches to configuration command mode for Ethernet interface 1/3 and applies the QoS queue list (QOS-LIST2) to the receiving side.

## 7.3 Operation

### 7.3.1 List of operation commands

The following table describes the operation commands for port shaper.

Table 7-9: List of operation commands

Command name	Description
show qos queueing port	Shows information about the port input and output queues.
clear qos queueing port	Clears the queue statistics displayed by the show qos queueing port command.

### 7.3.2 Checking scheduling

The following figure shows how to use the show qos queueing port command to check the result of scheduling, with an example of NL1G-12T as NIF.

Figure 7-5: Checking scheduling

```
> show qos queueing port 1/1 out
Date 20XX/08/01 12:00:00 UTC
NIF1/Port1 (out)
Max-queue=8, Schedule-mode=pq                                     <-1
Port-rate-limit=100Mbps, Active-rate=100Mbps
Queue1 : Qlen=0, Peak-Qlen=124, Limit-Qlen=511
         Drop-mode=tail-drop
Discard      Send packets      Discard packets      Send bytes
1             2248                0                    -
2              0                  0                    -
3              0                  0                    -
4              0                  0                    -
Total        2248                0                3372732
:
:
Queue8 : Qlen=0, Peak-Qlen=232, Limit-Qlen=511
         Drop-mode=tail-drop
Discard      Send packets      Discard packets      Send bytes
1              0                  0                    -
2            1528                0                    -
3              0                  0                    -
4              0                  0                    -
Total        1528                0                2292210
```

1. Make sure that the information for the Schedule-mode parameter shows the specified type of scheduling (in this example, pq).

### 7.3.3 Checking queue number specification

The following figure shows how to use the show qos queueing port command to check the configuration details for queue number specification, with an example of NL1G-12T as NIF.

Figure 7-6: Checking queue number specification

```
> show qos queueing port 1/11 out
Date 20XX/01/01 12:00:00 UTC
NIF1/Port11 (out)
Max-queue=4, Schedule-mode=pq                                     <-1
Port-rate-limit=100Mbps, Active-rate=100Mbps
Queue1 : Qlen=0, Peak-Qlen=172, Limit-Qlen=1023
         Drop-mode=tail-drop
Discard      Send packets      Discard packets      Send bytes
1             6225                0                    -
```

```

2                0                0                -
3                0                0                -
4                0                0                -
Total            6225            0                9207502
:
:
Queue4 : Qlen=0, Peak-Qlen=32, Limit-Qlen=1023
        Drop-mode=tail-drop
Discard    Send packets    Discard packets    Send bytes
1          0                0                -
2          1575            0                -
3          0                0                -
4          0                0                -
Total      1575            0                2262576

```

1. Make sure that the information for the `Max-queue` parameter shows the specified number of queues (in this example, 4).

### 7.3.4 Checking port bandwidth control

The following figure shows how to use the `show qos queueing port` command to check the configuration details for port bandwidth control, with an example of NL1G-12T as NIF.

*Figure 7-7: Checking port bandwidth control*

```

> show qos queueing port 1/12 out
Date 20XX /01/01 12:00:00 UTC
NIF1/Port12 (out)
Max-queue=8, Schedule-mode=pq
Port-rate-limit=20Mbps, Active-rate=20Mbps <-1
Queue1 : Qlen=0, Peak-Qlen=92, Limit-Qlen=511
        Drop-mode=tail_drop
Discard    Send packets    Discard packets    Send bytes
1          2248            0                -
2          0                0                -
3          0                0                -
4          0                0                -
Total      2248            0                3272162
:
:
Queue8 : Qlen=0, Peak-Qlen=86, Limit-Qlen=511
        Drop-mode=tail-drop
Discard    Send packets    Discard packets    Send bytes
1          0                0                -
2          1528            0                -
3          0                0                -
4          0                0                -
Total      1528            0                2292186

```

1. Make sure that the information for the `Port-rate-limit` parameter and `Active-rate` parameter shows the specified bandwidth value (in this example, 20 Mbit/s).

### 7.3.5 Checking queuing priority

Here, the queue number for the queued frames, queuing priority, and discarded packets are checked assuming that the traffic (traffic where a Qlen value of 511 for Queue8 is remaining) is forwarded in a port. The priority class is 8, and the discard class is 1 in the target QoS flow.

The following figure shows how to use the `show qos queueing port` command to check the configuration details for queuing priority, with an example of NL1G-12T as NIF.

*Figure 7-8: Checking queuing priority*

```

> show qos queueing port 1/11 out
Date 20XX/01/01 12:00:00 UTC
NIF1/Port11 (out)

```

```

Max-queue=8, Schedule-mode=pq
Port-rate-limit=100Mbps, Active-rate=100Mbps
Queue1 : Qlen=0, Peak-Qlen=0, Limit_Qlen=511
         Drop-mode=tail-drop
         Discard      Send packets      Discard packets      Send bytes
         1            0                0                    -
         2            0                0                    -
         3            0                0                    -
         4            0                0                    -
         Total        0                0                    0
         :
         :
Queue8 : Qlen=204, Peak-Qlen=204, Limit-Qlen=511
         Drop-mode=tail-drop
         Discard      Send packets      Discard packets      Send bytes
         1            6533              8245                -
         2            0                0                    -
         3            0                0                    -
         4            0                0                    -
         Total        6533              8245                9786580

```

- Make sure that the Qlen value for Queue8 has a count value.
- Make sure that the Qlen value is 40% of the Limit\_Qlen value and that the Discard1 counter for Discard packets has been incremented.

## 7.4 Correspondence between NIFs and port shapers

The following tables describe the correspondence between NIFs and each port shaper function.

*Table 7-10:* Correspondence between NIFs and port shapers (1/2)

Abbreviated name of NIF model	Scheduling				
	PQ	RR	4PQ+4WFQ	2PQ+4WFQ+2BEQ	4WFQ+4BEQ
NL1G-12T	Y	Y	Y	Y	Y
NL1G-12S	Y	Y	Y	Y	Y
NLXG-6RS	Y	Y	Y	Y	Y
NMCG-1C	Y	Y	--	--	--

*Table 7-11:* Correspondence between NIFs and port shapers (2/2)

Abbreviated name of NIF model	Queue number specification	Port bandwidth control	Drop control	
			Tail drop	Queuing priority
NL1G-12T	Y	Y	Y	4
NL1G-12S	Y	Y	Y	4
NLXG-6RS	Y	Y	Y	4
NMCG-1C	Y	Y	Y	4

Legend: Y: Supported, --: Not supported



## Chapter

---

# 8. Queues in the Device

---

This chapter describes the queues in the Device.

8.1 Description

8.2 Operation

## 8.1 Description

### 8.1.1 Overview

There are several kinds of queues in the Device. The following figures show the queues in the Device and the flow of frames.

Figure 8-1: Queues in the Device and the flow of frames (for frames that go through BCU-CPU)

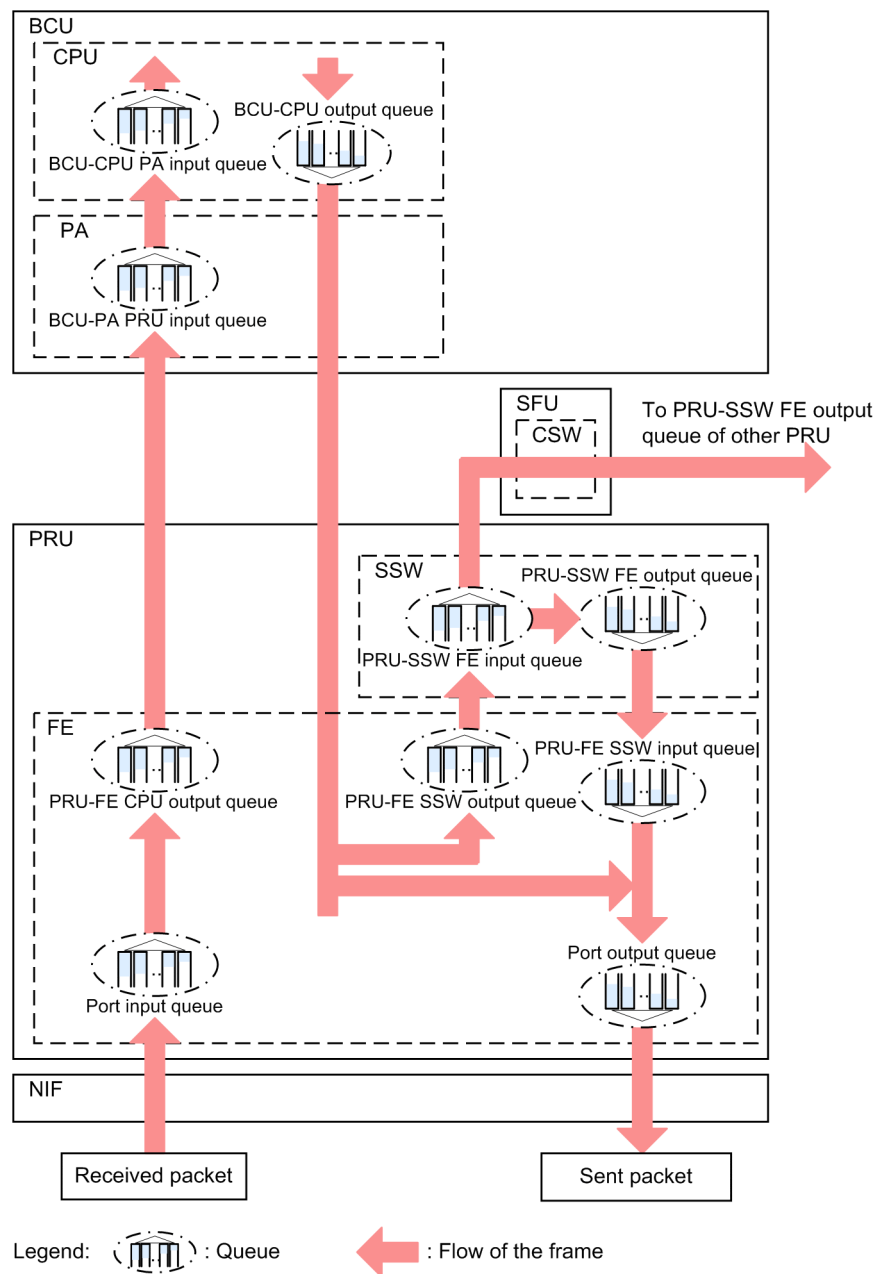
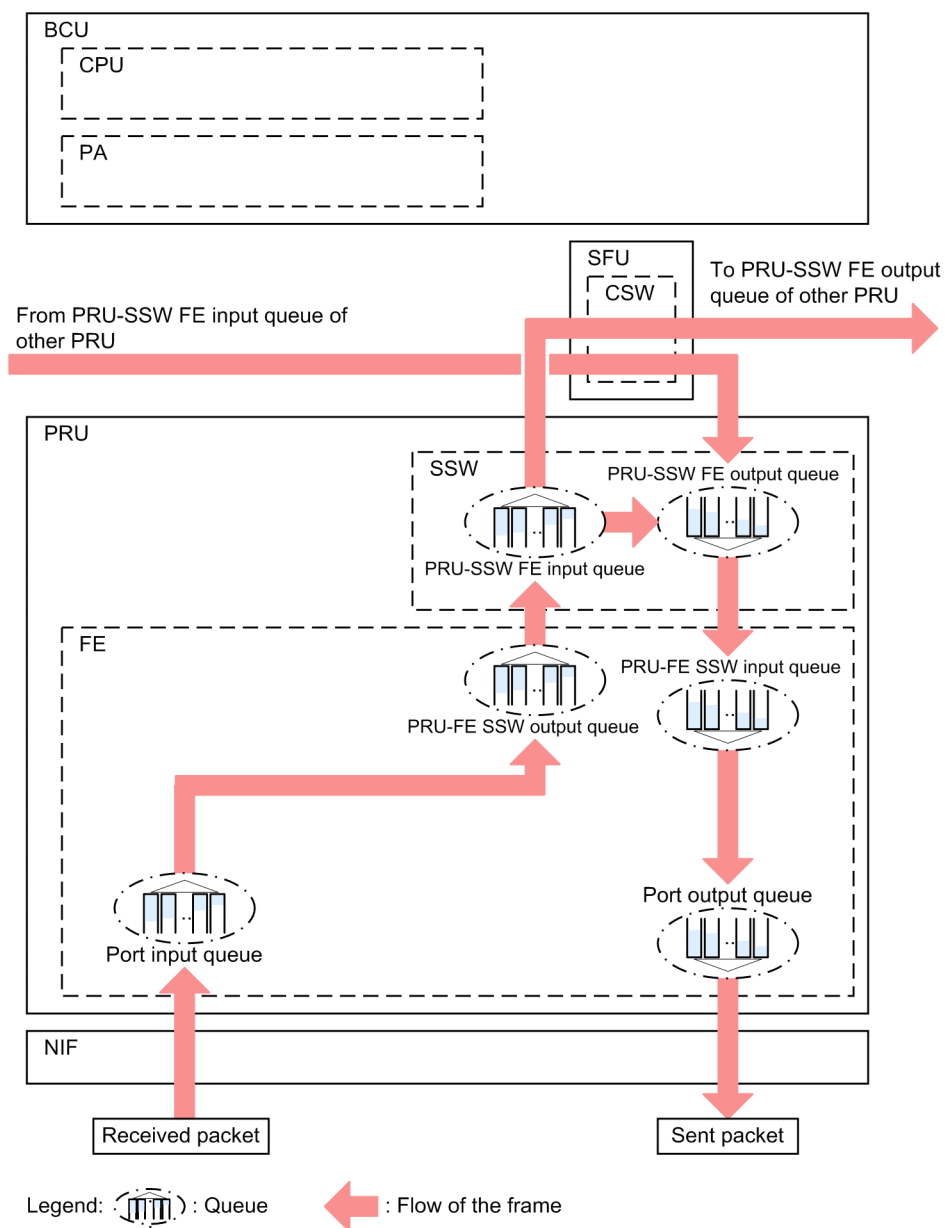


Figure 8-2: Queues in the Device and the flow of frames (for frames that do not go through BCU-CPU)



You can check the operating status and statistics for queues by using the `show qos queueing` operation command.

## 8.2 Operation

### 8.2.1 List of operation commands

The following table describes the operation commands for queues in the Device.

*Table 8-1:* List of operation commands

Command name	Description
show qos queueing	Shows all the queue information in the Device.
clear qos queueing	Clears all the queue statistics that are displayed by using the show qos queueing command.
show qos queueing bcu	Shows BCU queue information.
clear qos queueing bcu	Clears all the queue statistics that are displayed by using the show qos queueing bcu command.
show qos queueing pru	Shows PRU queue information.
clear qos queueing pru	Clears all the queue statistics that are displayed by using the show qos queueing pru command.
show qos queueing port	Shows information about the port input and output queues.
clear qos queueing port	Clears all the queue statistics that are displayed by using the show qos queueing port command.

### 8.2.2 Checking BCU queue information

You can check BCU queue information by using the show qos queueing bcu command. The following figure shows the result of executing the command.

*Figure 8-3:* Checking BCU queue information

```
> show qos queueing bcu cpu out
Date 20XX/01/01 12:00:00 UTC
BCU-CPU (Out)
Max-queue=8
Queue1 : Qlen=0, Limit-Qlen=256
          Send packets      Discard packets      Send bytes
Total              0              0              0
          :
          :
Queue8 : Qlen=147, Limit-Qlen=256
          Send packets      Discard packets      Send bytes
Total              8974655      0              2297566580
>
```

You can check the number of packets that accumulated in the BCU-CPU output queues by checking the value for Send packets, the number of discarded packets by checking the value for Discard packets, and the number of bytes for accumulated packets by checking the value for Send bytes.

### 8.2.3 Checking PRU queue information

You can check PRU queue information by using the show qos queueing pru command. The following figure shows the result of executing the command.

*Figure 8-4:* Checking PRU queue information

```
> show qos queueing pru 1 fe from-ssw control
Date 20XX/01/01 12:00:00 UTC
```

```

PRU1-FE (From-SSW Control)
Max-queue=8
Queue1 : Qlen=0, Peak-Qlen=0, Limit-Qlen=31
  Discard      Send packets      Discard packets      Send bytes
  1              0                  0                  -
  2              0                  0                  -
  3              0                  0                  -
  4              0                  0                  -
  Total         0                  0                  0
:
:
Queue8 : Qlen=0, Peak-Qlen=7, Limit-Qlen=31
  Discard      Send packets      Discard packets      Send bytes
  1              2023              0                  -
  2              0                  0                  -
  3              0                  0                  -
  4              0                  0                  -
  Total         2023              0                  1151320
>

```

You can check the number of packets that accumulated in the PRU-FE SSW input queues by checking the value for `Send packets`, the number of discarded packets by checking the value for `Discard packets`, and the number of bytes for accumulated packets by checking the value for `Send bytes`. Note that the values are displayed for queuing priorities (`Discard`) and for total number (`Total`).



## Chapter

---

# 9. Port Mirroring

---

The port mirroring functionality sends a copy of sent or received frames to the specified port. This chapter describes port mirroring and how to use it.

9.1 Description

9.2 Configuration

## 9.1 Description

### 9.1.1 Overview of port mirroring

Port mirroring is functionality that sends a copy of sent or received frames to the specified port. The copying of frames is called mirroring. By using an analyzer to receive the forwarded mirror frames, you can monitor or analyze traffic.

The following figures show the flow of received frames and sent frames when mirroring is used.

Figure 9-1: Mirroring of received frames

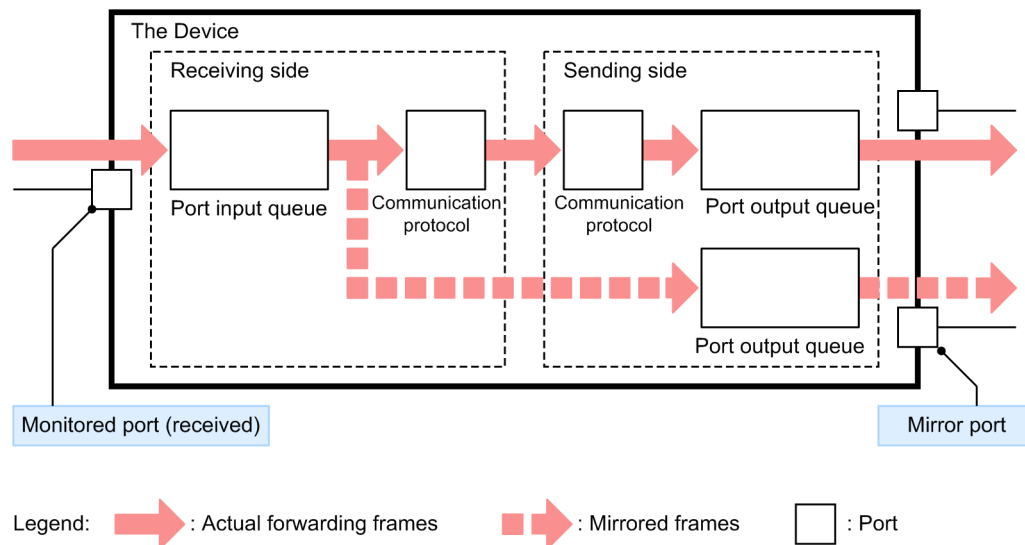
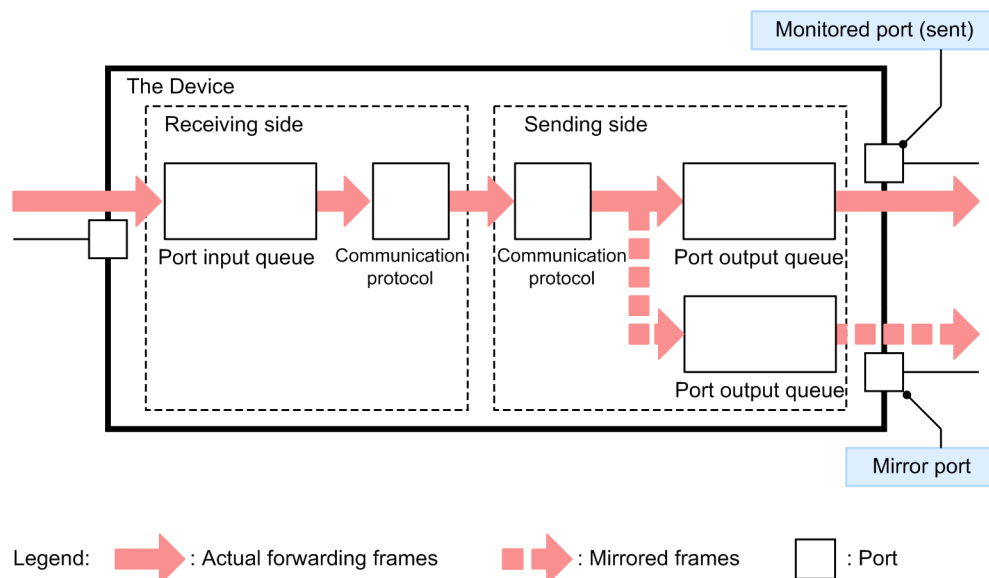


Figure 9-2: Mirroring of sent frames



As indicated in the above figures, a physical port whose traffic is monitored is called a monitored port, and the physical port to which the frames copied for mirroring are sent is called a mirror port.

In port mirroring for the received frames in the Device, the frames are copied immediately after they are output from the port input queues. In port mirroring for the sent frames in the Device, the frames are copied before they are queued to the port output queues.



## 9.1.2 Port mirroring specifications

### (1) *Basic specifications*

Every port except a port specified as a mirror port can be specified as a monitored port. Even if a port is specified as a monitored port, port functionality or interface functionality is not restricted.

For a mirror port, specify the port to which an analyzer is connected for monitoring or analyzing the traffic. A mirror port is used exclusively for port mirroring.

The combination of a monitored port and a mirror port is called a monitored session. Multiple monitored sessions can be defined for the Device.

In a monitored session, mirroring is performed for the received frames, sent frames, or both frames on the monitored port. The frames received at and sent from the monitored port can be sent to different mirror ports respectively. However, they cannot be sent to multiple mirror ports.

Also, note that the monitored and mirror ports can be set in a multipoint-to-point relationship. With the setting, copies of frames received at and sent from multiple monitored ports can be sent to a single mirror port. Furthermore, ports with different transmission speeds can be set separately for a monitored port and mirror port.

In the Device, mirrored frames are sent within the bandwidth specified to the mirror port. Note that mirrored frames that exceed the mirror port bandwidth are discarded.

### (2) *Mirror port specifications*

You can use Ethernet functionality such as auto-negotiation or flow control for the mirror port. However, the functionality of Layer 2 cannot be used, and thus the functionality such as CFM cannot be used for the mirror port.

Also, you cannot specify IP address, subinterface, or link aggregation for the mirror port. That is, a mirror port cannot be used as an IP interface.

Note that if you apply filter and QoS control to the mirror port, the mirrored frames are excluded from the targets of the policer, the marker, or priority changes by filter and QoS flow. However, mirrored frames are the target of drop control by port shaper, scheduling, and port bandwidth control.

### (3) *Mirroring of received frames*

All the frames received at monitored ports are mirrored. However, if there is an anomaly in the received frame, the frame is not mirrored.

### (4) *Mirroring of sent frames*

All the frames sent from monitored ports are mirrored. Note that the frames to be discarded due to congestion at the monitored port might be mirrored, and the frames sent from the monitored port might not be mirrored due to the congestion at the mirror port.

If you apply drop control by port shaper, scheduling, and port bandwidth control to the monitored port, the frames before the port shaper application are mirrored in the port mirroring for sent frames. That is, there are cases where a frame to be discarded at the monitored port is mirrored, or the order of sending frames is incoherent between the monitored and mirror ports.

## 9.1.3 Notes on using port mirroring

### (1) *Notes on mirroring sent frames*

If the monitored port and mirror port use different PRUs, the mirroring processing performance of the monitored port side PRU is limited to about 19 Mpacket/s. Note that this limitation does not apply to the normal packet forwarding.

## 9.2 Configuration

### 9.2.1 List of configuration commands

The following table describes the configuration commands for port mirroring.

*Table 9-1:* List of configuration commands

Command name	Description
monitor session	Configures port mirroring.

### 9.2.2 Configuring port mirroring

When port mirroring is configured, a combination of monitored ports and a mirror port is defined as a monitored session.

A session number is specified when an existing session is deleted. If an existing session number is specified, the existing session definition corresponding to the specified session number is overwritten by the new definition.

Ports used for normal data communication are specified as monitored ports. A port to which an analyzer is connected for monitoring or analyzing the traffic is specified as a mirror port. Note that the use of the mirror port is limited to communication of data copied for port mirroring.

#### (1) Mirroring of received frames

Points to note

The mirroring of sent or received frames can be defined for Ethernet interfaces. Specify separate Ethernet interfaces even if link aggregation is used. Also, you need to specify a port without an IP address, subinterface, or link aggregation as a mirror port.

Command examples

1. **(config)# monitor session 2 source interface gigabitethernet 1/1 rx destination interface gigabitethernet 1/5**

Connects the analyzer to port 1/5 and activates mirroring for the frames received at the port 1/1. The number of the monitored session to be used is 2.

#### (2) Mirroring of sent frames

Points to note

The mirroring of sent or received frames can be defined for Ethernet interfaces. Specify separate Ethernet interfaces even if link aggregation is used. Also, you need to specify a port without an IP address, subinterface, or link aggregation as a mirror port.

Command examples

1. **(config)# monitor session 1 source interface gigabitethernet 1/2 tx destination interface gigabitethernet 1/6**

Connects the analyzer to port 1/6 and activates mirroring for the frames sent from port 1/2. The number of the monitored session to be used is 1.

#### (3) Mirroring of sent or received frames

Points to note

The mirroring of sent or received frames can be defined for Ethernet interfaces. Specify

separate Ethernet interfaces even if link aggregation is used. Also, you need to specify a port without an IP address, subinterface, or link aggregation as a mirror port.

#### Command examples

1. `(config)# monitor session 1 source interface gigabitethernet 1/3 both destination interface gigabitethernet 1/11`

Connects the analyzer to port 1/11 and activates mirroring for the frames received and sent on port 1/3. The number of the monitored session to be used is 1.

#### **(4) Mirroring of sent or received frames to another port**

##### Points to note

The separate ports for mirroring of frames received at and sent from the monitored port are set.

#### Command examples

1. `(config)# monitor session 1 source interface gigabitethernet 1/3 rx destination interface gigabitethernet 1/11`  
`(config)# monitor session 2 source interface gigabitethernet 1/3 tx destination interface gigabitethernet 1/12`

Sets the destination for mirroring of the frame received at port 1/3 to port 1/11, and that of the frame sent from port 1/3 to port 1/12. The numbers of the monitored sessions to be used are 1 and 2.



## Chapter

---

# 10. sFlow Statistics (Flow Statistics) Functionality

---

This chapter describes the sFlow statistics functionality, which analyzes the traffic characteristics of packets forwarded by the Device, and how to use it

- 10.1 Description
- 10.2 Configuration
- 10.3 Operation

## 10.1 Description

### 10.1.1 Overview of sFlow statistics

The sFlow statistics functionality uses a relay device (such as a router or a switch) to monitor traffic across networks to analyze end-to-end traffic (flow) characteristics or the traffic characteristics of the neighboring networks. sFlow is a publicly available flow statistics protocol (RFC 3176) that supports statistics on Layer 2 to Layer 7. A device that receives and displays sFlow statistics (referred to hereafter as sFlow packets) is called an sFlow collector (referred to hereafter as collector). A device that sends sFlow packets to collectors is called an sFlow agent (referred to hereafter as agent). The following figure shows an example of a network configuration that uses sFlow statistics.

Figure 10-1: Example of a network configuration using sFlow statistics

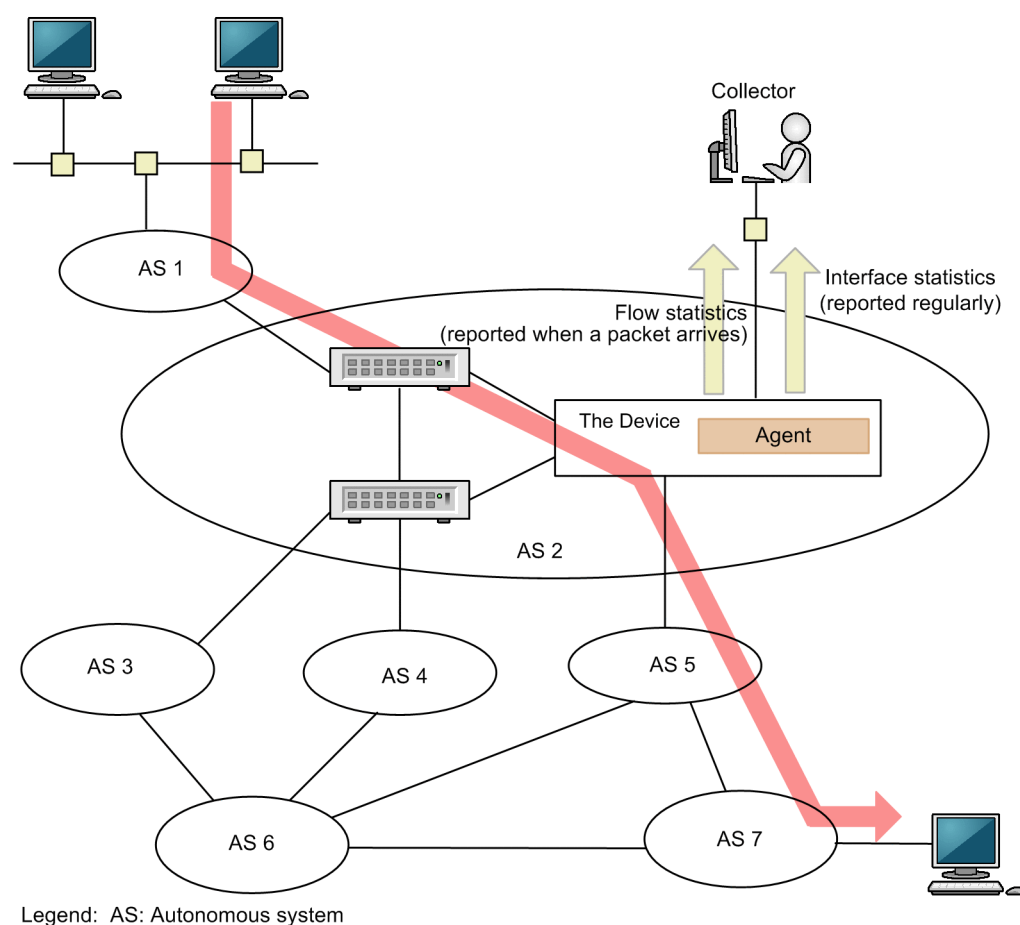
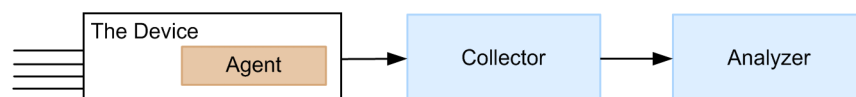


Figure 10-2: System configuration



Information monitored by an agent on the Device is collected by a collector, and the statistical results are displayed graphically by an analyzer. Accordingly, use of the sFlow statistics functionality requires a collector and an analyzer.

Table 10-1: Components required for system configuration

Parameters	Role
Agent (Device)	Collects statistics and sends it to a collector.
Collector <sup>#</sup>	Aggregates, edits, and displays statistics sent from an agent. The collector also sends edited data to an analyzer.
Analyzer	Graphically displays data sent from a collector.

<sup>#</sup>: The collector can sometimes be combined with the analyzer.

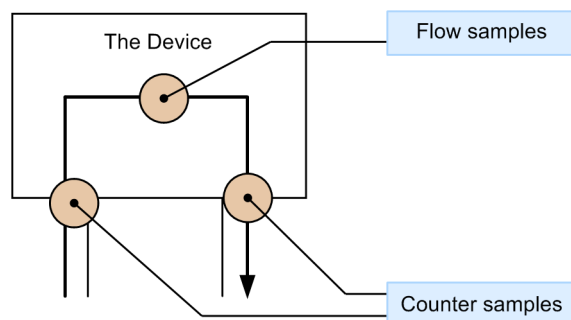
### 10.1.2 sFlow statistic agent functionality

An agent on the Device consists of the following two types of functionality:

- Flow statistics creation. (Because flow statistics are called flow samples in sFlow statistics, the term "flow sample" will be used hereafter.)
- Interface statistics creation. (Because interface statistics are called counter samples in sFlow statistics, the term "counter sample" will be used hereafter.)

The flow sample creation functionality samples sent and received packets (frames) at a user-specified rate, processes the packet information, and then sends it to a collector in flow sample format. The counter sample creation functionality sends interface statistics to a collector in counter sample format. The following figure shows collection points and collected data for the functionality.

Figure 10-3: Flow sample and counter sample



Flow sample (flow statistics)

Analysis of traffic characteristics (from where and to where the types of traffic are forwarded)

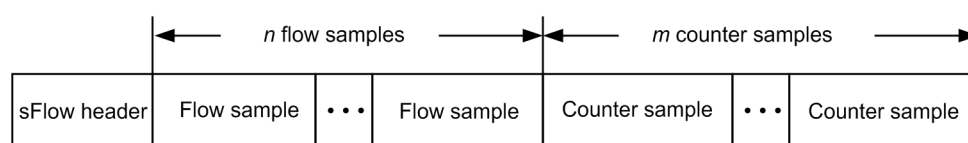
Counter samples (interface statistics)

Analysis of events occurring on interfaces (number of send and receive counter errors = MIB information equivalent)

### 10.1.3 sFlow packet format

This section describes sFlow packets (flow sample and counter sample) that the Device sends to a collector. The format used to send the packets to a collector is defined in RFC 3176. The following figure shows the sFlow packet format.

Figure 10-4: sFlow packet format



Note that, in the Device, a flow sample and counter sample will never be included in an sFlow packet at the same time.

### (1) sFlow header

The following table describes information set in the sFlow header.

Table 10-2: sFlow header format

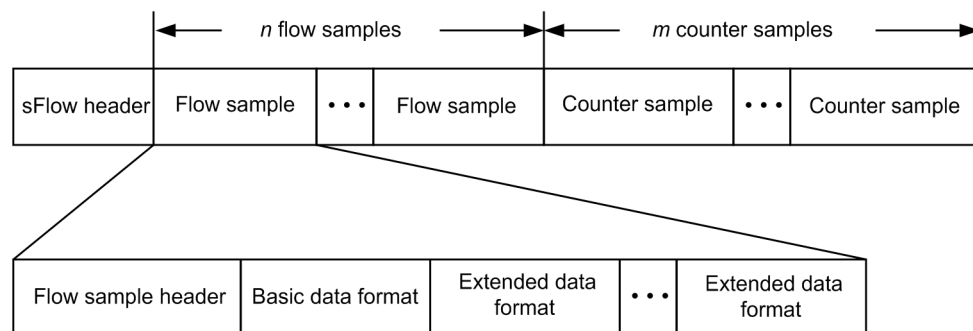
Configuration items	Description	Supported
Version number	sFlow packet version (Version 4 is supported.)	Y
Address type	IP type of the agent (1 is IPv4, and 2 is IPv6)	Y
Agent IP address	Agent IP address	Y
Sequence number	Number incremented each time an sFlow packet is generated	Y
Generation time	Time in milliseconds since the device started	Y
Number of samples	Number of sampled (flow and counter) packets contained in the signal. ( $n + m$ is set in the example in Figure 10-4: sFlow packet format.)	Y

Legend: Y: Supported

### (2) Flow sample

A flow sample is the format used to retrieve packets from among the received packets that are to be forwarded to another device or sent to the Device at a specified sampling interval for transmission to a collector. Because the flow sample functionality collects information about the monitored packets and information that is not contained in a packet (such as the receiving interface, sending interface, and the AS number), detailed network monitoring becomes possible. The following figure shows the flow sample format.

Figure 10-5: Flow sample format



#### (a) Flow sample header

The following table describes the information set in the flow sample header.

Table 10-3: Flow sample header format

Configuration items	Description	Supported
sequence_number	Number incremented each time a flow sample is generated	Y
source_id	SNMP Interface Index, which indicates the source on a device from which the flow sample was created (receiving interface) If the interface is unknown, 0 is set.	Y



Configuration items	Description	Supported
sampling_rate	Sampling rate of flow samples	Y
sample_pool	Total number of packets arriving at an interface	Y
drops	Total number of flow samples lost due to resource shortages. Fixed to 0 in the Device.	Y
input	SNMP Interface Index of a receiving interface. If the interface is unknown, 0 is set. (same as source_id)	Y
output	SNMP Interface Index <sup>#1</sup> of a sending interface. If the sending interface is unknown, 0 is set. If multiple sending interfaces are used (such as in multicasting), the highest bit is set to 1, and the lower bits represent the number of sending interfaces. <sup>#2</sup>	Y

Legend: Y: Supported

#1: In case of software forwarding, 0 can be set.

#2: The lower bits are set to 0 because the multiple interfaces are not supported.

#### (b) Basic data format

There are three basic data format types (header, IPv4, and IPv6), but only one can be set. By default, the header type is set as the basic data type. If you want to use the IPv4 type or the IPv6 type, use a configuration command to change the setting. The following tables describe the formats.

Table 10-4: Header type format

Configuration items	Description	Supported
packet_information_type	Basic data format type (header type is 1) <sup>#</sup>	Y
header_protocol	Header protocol number (ETHERNET is 1)	Y
frame_length	Length of the original packet	Y
header_length	Length of a packet as sampled (default length is 128)	Y
header◇	Contents of the sampled packet	Y

Legend: Y: Supported

#: This format is used if a packet cannot be analyzed as an IP packet.

Table 10-5: IPv4 type format

Configuration items	Description	Supported
packet_information_type	Basic data format type (IPv4 type is 2)	Y
length	Length of the IPv4 packet	Y
protocol	IP protocol type (TCP is 6 and UDP is 17, for example)	Y
src_ip	Source IP address	Y
dst_ip	Destination IP address	Y
src_port	Source port number	Y
dst_port	Destination port number	Y

Configuration items	Description	Supported
tcp_flags	TCP flag	Y
TOS	IP TOS (type of service)	Y

Legend: Y: Supported

Table 10-6: IPv6 type format

Configuration items	Description	Supported
packet_information_type	Basic data format type (IPv6 type is 3)	Y
length	Length of the IPv6 packet excluding the lower layers	Y
protocol	IP protocol type (TCP is 6 and UDP is 17, for example)	Y
src_ip	Source IP address	Y
dst_ip	Destination IP address	Y
src_port	Source port number	Y
dst_port	Destination port number	Y
tcp_flags	TCP flag	Y
priority	Priority	Y

Legend: Y: Supported

### (c) Extended data format

There are five types of extended data formats: switch type, router type, gateway type, user type, and URL type. By default, the extended data format is configured to collect all the extended data formats except the switch type, and send them to a collector. You can change this format in the configuration. The following tables describe the formats.

Table 10-7: List of extended data formats

Extended data format	Description	Supported
Switch type	Collects switch information (such as VLAN information).	N
Router type	Collects router information (such as NextHop).	Y
Gateway type	Collects gateway information (such as AS number).	Y
User type	Collects user information (such as TACACS or RADIUS information).	Y
URL type	Collects URL information.	Y

Legend: Y: Supported, N: Not supported

Table 10-8: Router type format

Configuration items	Description	Supported
extended_information_type	Extended data format type (router type is 2)	Y
nexthop_address_type	IP address type of the next forward destination	Y <sup>#</sup>
nexthop	IP address of the next forward destination router	Y <sup>#</sup>

Configuration items	Description	Supported
src_mask	Prefix mask bit of the source address	Y
dst_mask	Prefix mask bit of the destination address	Y

Legend: Y: Supported

#: Collected at 0 if the destination address is a group address.

Table 10-9: Gateway type format

Configuration items	Description	Supported
extended_information_type	Extended data format type (gateway type is 3)	Y
as	AS number of the Device	Y
src_as	AS number of the source	Y <sup>#1</sup>
src_peer_as	Neighboring AS number to the source	Y <sup>#1, #2</sup>
dst_as_path_len	Number of AS information items (fixed at 1)	Y
dst_as_type	Type of the AS path (2 is AS_SEQUENCE)	Y
dst_as_len	Number of ASs (fixed at 2)	Y
dst_peer_as	Neighboring AS number to the destination	Y <sup>#1</sup>
dst_as	AS number of the destination	Y <sup>#1</sup>
communities◇	Community for the route <sup>#3</sup>	N
localpref	Local priority about this route <sup>#3</sup>	N

Legend: Y: Supported, N: Not supported

#1: If the path to the sending and receiving destination is a direct route, the AS number is recorded as 0.

#2: This field includes the value used as the neighboring AS number when packets are sent from the Device to the source device. This number might be different from the neighboring AS number of the device to which the packet was actually forwarded before reaching the Device.

#3: Fixed at 0 because the item is not supported.

Table 10-10: User type format

Configuration items	Description	Supported
extended_information_type	Extended data format type (user type is 4) <sup>#1</sup>	Y
src_user_len	Length of the user name of the source	Y
src_user◇	User name of the source	Y
dst_user_len	Length of the user name of the destination <sup>#2</sup>	N
dst_user◇	User name of the destination <sup>#2</sup>	N

Legend: Y: Supported, N: Not supported

#1: The destination UDP port number 1812 for RADIUS, and the destination port number 49 for

TACACS are collected.

#2: Fixed at 0 because the item is not supported.

Table 10-11: URL type format

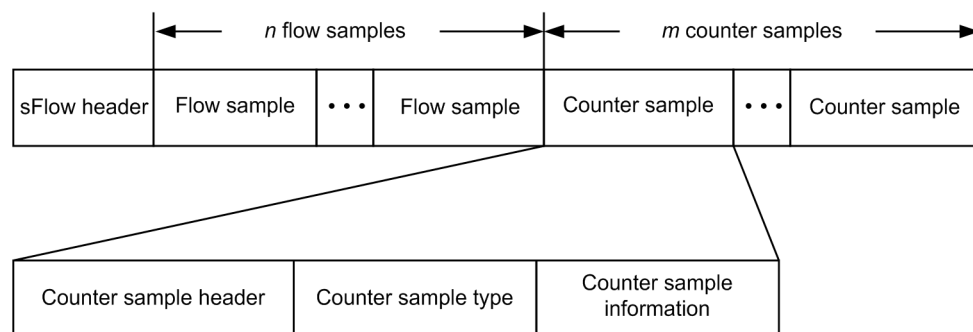
Configuration items	Description	Supported
extended_information_type	Extended data format type (URL type is 5)	Y
url_direction	URL information source (The source address is 1, and the destination address is 2.)	Y
url_len	URL length	Y
url◇	Contents of the URL	Y

Legend: Y: Supported

### (3) Counter sample

A counter sample sends interface statistics (number of arrived packets and number of errors). The format to be sent to a collector is determined according to the interface type. The following figure shows the counter sample format.

Figure 10-6: Counter sample format



#### (a) Counter sample header

The following table describes the information set in the counter sample header.

Table 10-12: Counter sample header format

Configuration items	Description	Supported
sequence_number	Number incremented each time a counter sample is generated	Y
source_id	The SNMP Interface Index, which indicates the source (specific port) on a device the counter sample	Y
sampling_interval	Interval at which counter samples are sent to a collector	Y

Legend: Y: Supported

#### (b) Counter sample type

The counter sample types reflect interface types and are collected according to this classification. The following table describes the items set as a counter sample type.

Table 10-13: List of counter sample types

Configuration items	Description	Supported
GENERIC	General statistics (counters_type is 1)	N <sup>#1</sup>
ETHERNET	Ethernet statistics (counters_type is 2)	Y
TOKENRING	Token ring statistics (counters_type is 3)	N <sup>#2</sup>
FDDI	FDDI statistics (counters_type is 4)	N <sup>#2</sup>
100BaseVG	VG statistics (counters_type is 5)	N <sup>#2</sup>
WAN	WAN statistics (counters_type is 6)	N <sup>#2</sup>
VLAN	VLAN statistics (counters_type is 7)	N <sup>#2</sup>

Legend: Y: Supported, N: Not supported

#1: Information relating to GENERIC is included in the format of the ETHERNET type.

#2: The interface types are not supported by the Device.

### (c) Counter sample information

Counter sample information to be collected varies according to the counter sample type. Except for VLAN statistics, information is sent according to the statistics (RFC) used by MIBs. The following table describes items set as counter sample information.

Table 10-14: Counter sample information

Configuration items	Description	Supported
GENERIC	General statistics (see RFC 2233)	N
ETHERNET	Ethernet statistics (see RFC 2358)	Y <sup>#</sup>
TOKENRING	Token ring statistics (see RFC 1748)	N
FDDI	FDDI statistics (see RFC 1512)	N
100BaseVG	VG statistics (see RFC 2020)	N
WAN	WAN statistics (see RFC 2233)	N
VLAN	VLAN statistics	N

Legend: Y: Supported, N: Not supported

#: Among the Ethernet statistics, ifDirection and dot3StatsSymbolErrors cannot be collected.

## 10.1.4 Behavior of sFlow statistics on a Device

### (1) Notes on the packets to be collected for sFlow statistics

- In the Device, received packets are collected for flow samples.
- The packets subject to discarding when they were received (such as packets selected by the filter functionality for discarding) are handled as out-of-scope packets. However, the packets that are discarded when queued according to the drop control of QoS functionality at the sending side are collected for flow samples.

### (2) Notes on the locations for collecting flow sample data

- The contents of a flow sample packet when it enters the Device are collected. (The contents

are not reflected in sFlow packets even after conversion on the Device.)

- In flow sampling on the Device, received packets are sampled and sent to a collector. Accordingly, packets are sent to a collector as they are being forwarded even if they are subject to discarding when the filter functionality or the QoS functionality is configured on the sending side. If you also use the filter functionality or the QoS functionality, check the conditions for discarding packets before starting operation. The following table and figure describe the flow sample collection conditions when flow sampling is used with other functionality.

*Table 10-15:* Flow sample collection conditions when flow sampling is used with other functionality

Functionality	When received packets are collected for a flow sample
Filter functionality (receiving side)	Not counted even if the packet to be discarded
QoS functionality (policer) (receiving side)	Not counted even if the packet to be discarded
Filter functionality (sending side) <sup>#1</sup>	Counted even if the packets are to be discarded.
QoS functionality (policer and shaper) (sending side) <sup>#1</sup>	Counted even if the packets are to be discarded.
uRPF functionality	Not counted if the packets are to discarded.
Incoming	Collected
Outgoing (such as ping from the Device)	--
Policy-based routing	Collected <sup>#2, #3</sup>

Legend: --: Not applicable

#1

The Device collects the contents of all packets at the time the packets enter the Device.

#2

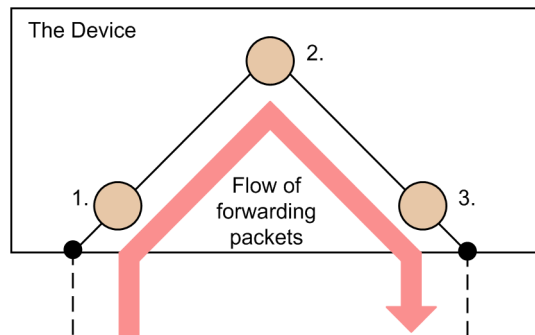
The following information is the routing information of the forwarding destination according to the routing protocol, instead of the routing information of the forwarding destination based on the policy base routing.

- nexthop and dst\_mask of router type formats
- dst\_peer\_as and dst\_as of gateway type formats

#3

Packets discarded by the deny specification in the default operation are also collected.

*Figure 10-7:* Location for determining flow sampling targets when used with other functionality



1. Filter functionality check for receiving side or QoS functionality check for receiving side
2. Determination of whether received packets are to be collected for a flow sample
3. Filter functionality check for sending side or QoS functionality check for sending side

**(3) Packets to be collected for a counter sample**

- In the Device, received packets and sent packets are collected for a counter sample.

## 10.2 Configuration

### 10.2.1 List of configuration commands

The following table describes the configuration commands for sFlow statistics.

*Table 10-16:* List of configuration commands

Command name	Description
sflow additional-http-port	Sets the port number used for HTTP packets to a port number other than 80 when URL information is used in the extended data format.
sflow destination	Specifies the IP address of the collector, which is the destination for sFlow packets.
sflow extended-information-type	Sets whether to send flow samples in an extended data format.
sflow forward ingress	Causes the received traffic of the specified port to be monitored by the flow sample. Also, causes the sent and received traffic of the specified port to be monitored by the counter sample.
sflow max-header-size	If the header type is used for the basic data format, this command sets the maximum size of a header to be copied, starting from the beginning of the sample packet.
sflow max-packet-size	Sets the sFlow packet size.
sflow packet-information-type	Sets the basic data format of the flow sample.
sflow polling-interval	Specifies the interval for sending counter samples to the collector.
sflow sample	Sets the sampling interval applying to the entire device.
sflow source	Specifies the IP address to be configured as the sFlow packet source (agent).

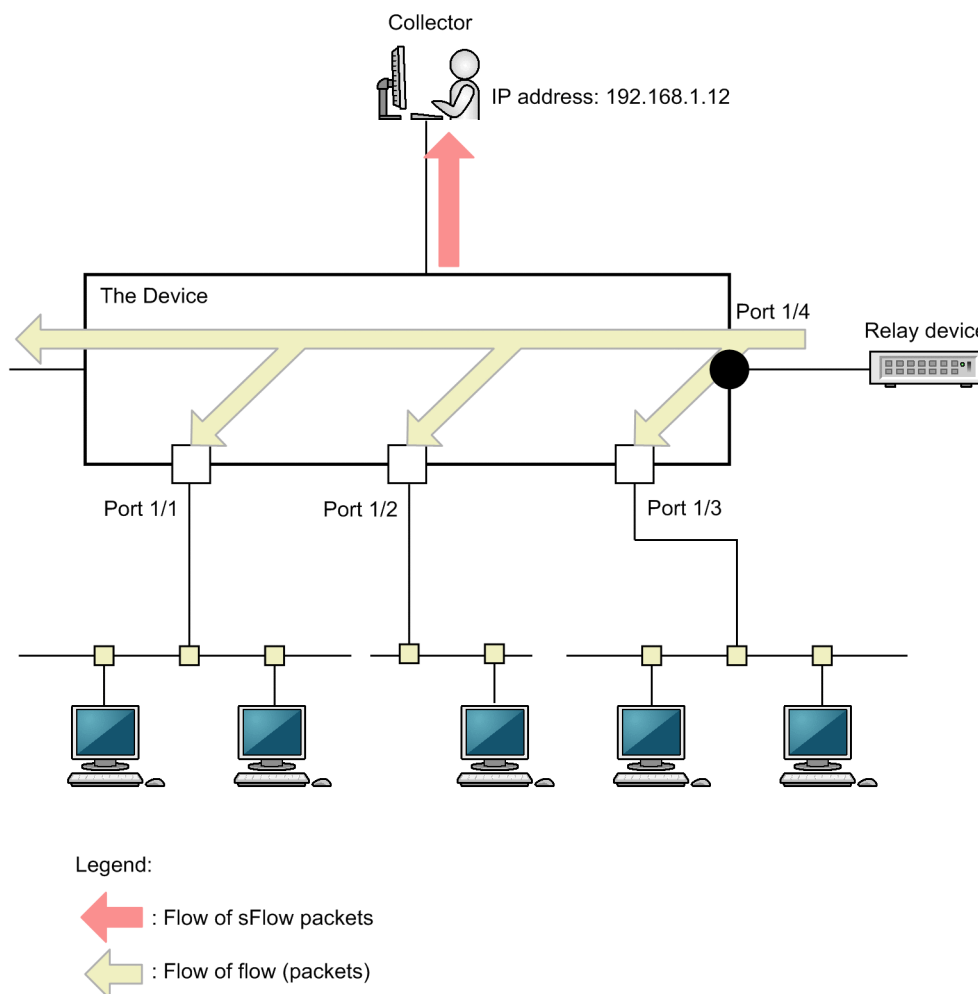
### 10.2.2 Configuring basic settings for the sFlow statistics functionality

#### (1) Configuration for monitoring received packets

The following figure shows an example of a configuration for monitoring received packets on port 1/4.



Figure 10-8: Example configuration for monitoring received packets on port 1/4



#### Points to note

Two separate configurations are required: one configuration is enabled for the entire device, and the other configuration is used to specify a port that is actually used.

#### Command examples

1. **(config)# sflow destination 192.168.1.12**

Sets 192.168.1.12 as the IP address of the collector.

2. **(config)# sflow sample 512**

Monitors the traffic every 512 packets.

3. **(config)# interface gigabitethernet 1/4**

Switches to the configuration command mode for port 1/4.

4. **(config-if)# sflow forward ingress**

Activates the flow sample creation functionality for the received packets and the counter sample creation functionality for the packets sent and received on port 1/4.

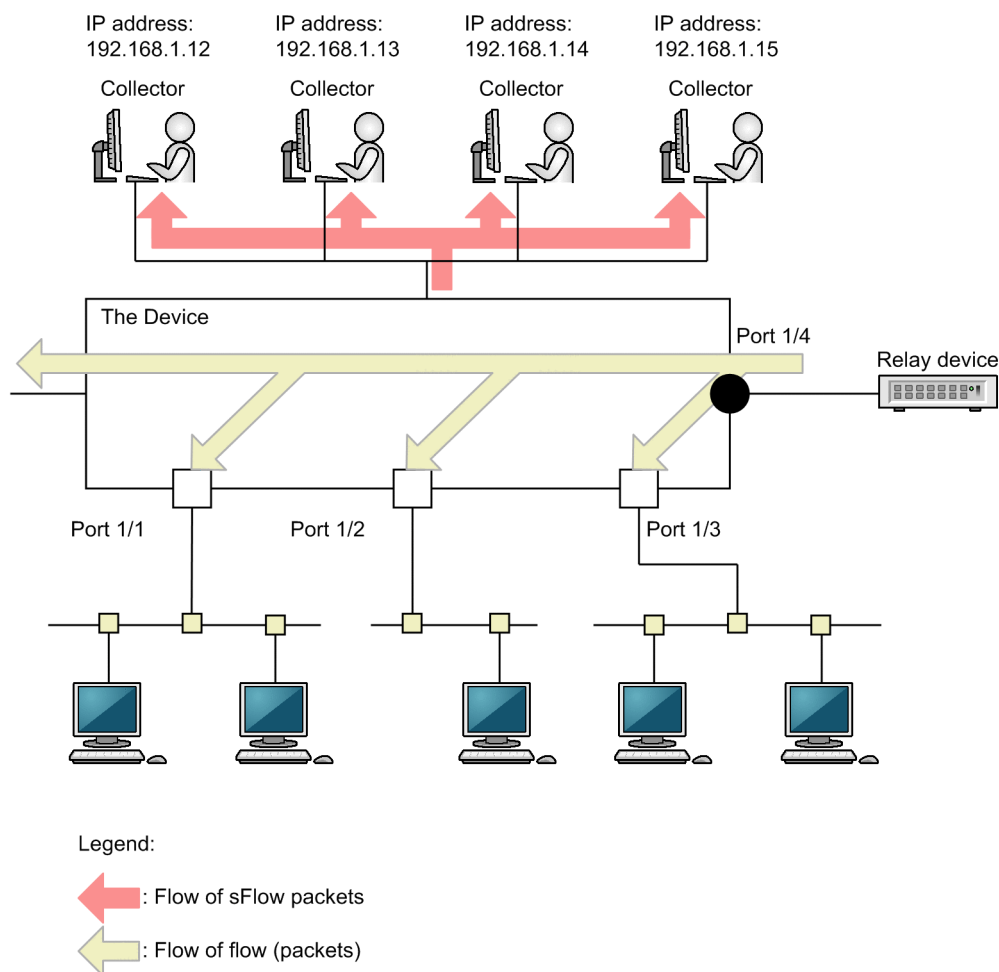
## Notes

The sampling interval that can be specified by the `sflow sample` command must be determined with the amount of packet flow (packet/s) taken into consideration. For details, see `sflow sample` in the manual *Configuration Command Reference Vol. 2 For Version 12.1*.

### (2) Configuration for connecting with multiple collectors

The following figure shows an example of a configuration for connecting the Device with four collectors.

Figure 10-9: Example of a configuration for connecting the Device with four collectors



## Points to note

Multiple (maximum of four) collectors can be connected for backup.

## Command examples

1. **(config)# sflow destination 192.168.1.12**  
Sets 192.168.1.12 as the IP address of the collector.
2. **(config)# sflow destination 192.168.1.13**  
Sets 192.168.1.13 as the IP address of the collector.

3. **(config)# sflow destination 192.168.1.14**

Sets 192.168.1.14 as the IP address of the collector.

4. **(config)# sflow destination 192.168.1.15**

Sets 192.168.1.15 as the IP address of the collector.

5. **(config)# sflow sample 512**

Monitors the traffic every 512 packets.

6. **(config)# interface gigabitethernet 1/4**

Switches to the configuration command mode for port 1/4.

7. **(config-if)# sflow forward ingress**

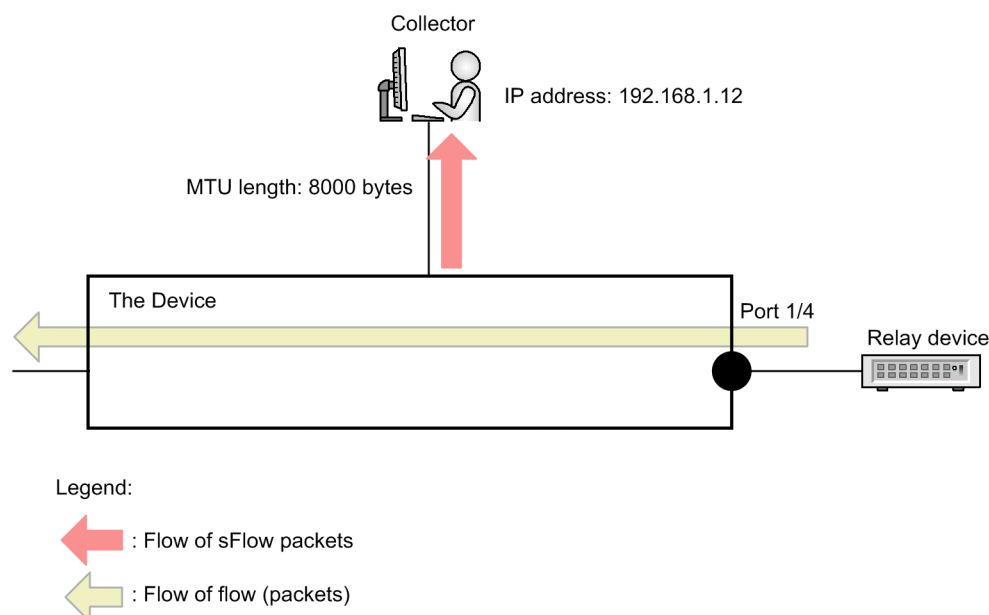
Activates the flow sample creation functionality for the received packets and the counter sample creation functionality for the packets sent and received on port 1/4.

### 10.2.3 Configuration example for the sFlow statistics configuration parameter

#### (1) Adjusting the MTU length and the sFlow packet size

The following figure shows an example of a configuration to adjust the size of sFlow packet to be sent to the collector when a line with an MTU length of 8000 bytes is connected to the collector.

Figure 10-10: Example when the MTU value of the line to the collector is set to 8000 bytes



#### Points to note

By default, sFlow packets with a maximum of 1400 bytes are sent to a collector. If the MTU value of the line to the collector is large, adjust the packet size to the same size as the MTU value so that packets can be sent efficiently to the collector.

#### Command examples

1. **(config)# sflow destination 192.168.1.12**  
Sets 192.168.1.12 as the IP address of the collector.
2. **(config)# sflow sample 32**  
Monitors the traffic every 32 packets.
3. **(config)# sflow max-packet-size 8000**  
Sets the maximum sFlow packet size to 8000 bytes.
4. **(config)# interface gigabitethernet 1/4**  
Switches to the configuration command mode for port 1/4.
5. **(config-if)# sflow forward ingress**  
Activates the flow sample creation functionality for the received packets and the counter sample creation functionality for the packets sent and received on port 1/4.

#### **(2) Narrowing down the information to be collected**

The following describes an example of a configuration when only IP address information is needed.

##### Points to note

All information about sFlow packets is collected by the default configuration. If you want to decrease CPU usage, you can change the configuration settings so that unnecessary information will not be collected.

#### Command examples

1. **(config)# sflow destination 192.168.1.12**  
Sets 192.168.1.12 as the IP address of the collector.
2. **(config)# sflow sample 512**  
Monitors the traffic every 512 packets.
3. **(config)# sflow packet-information-type ip**  
Sets the IP format as the basic data format for flow samples.
4. **(config)# sflow extended-information-type router**  
Sets the router format as the extended data format for flow samples (only router information can be retrieved).
5. **(config)# interface gigabitethernet 1/4**

Switches to the configuration command mode for port 1/4.

6. **(config-if)# sflow forward ingress**

Activates the flow sample creation functionality for the received packets and the counter sample creation functionality for the packets sent and received on port 1/4.

### **(3) Fixing the agent IP address of sFlow packets**

The following describes an example of a configuration for sending packets to a collector by using the IP address assigned to the loopback interface as the agent IP address.

#### **Points to note**

A normal collector determines if a device is the same device based on the agent IP address contained in an sFlow packet. Therefore, if the agent IP address is not set by using the `sflow source` command or the `interface loopback` command, the collector might display the status as if packets had been sent from multiple devices. To see long-term information, fix the agent IP address.

#### **Command examples**

1. **(config)# interface loopback 0**

Switches to configuration command mode for the loopback interface.

2. **(config-if)# ip address 192.168.1.1**

Sets 192.168.1.1 as the IPv4 address of the loopback interface.

3. **(config-if)# ipv6 address 2001:db8:811:ff00::1**  
**(config-if)# exit**

Sets 2001:db8:811:ff00::1 as the IPv6 address of the loopback interface.

4. **(config)# sflow destination 192.168.1.12**

Sets 192.168.1.12 as the IP address of the collector.

5. **(config)# sflow sample 512**

Monitors the traffic every 512 packets.

6. **(config)# interface gigabitethernet 1/4**

Switches to the configuration command mode for port 1/4.

7. **(config-if)# sflow forward ingress**

Activates the flow sample creation functionality for the received packets and the counter sample creation functionality for the packets sent and received on port 1/4.

#### **Notes**

If you use the loopback interface IP address, the configuration by the `sflow source` command is not needed. If the IP address is specified by using the `sflow source` command, then the specified IP address takes priority.

#### **(4) Collecting URL information in a local network environment**

The following describes an example of a configuration when port 8080 is used for HTTP packets in a local network environment.

##### **Points to note**

When URL information (HTTP packets) is collected by using the sFlow statistics functionality on the Device, the default destination port number is set to 80. If the port number is different within the local network, add and specify a port number.

##### **Command examples**

1. **(config)# sflow destination 192.168.1.12**

Sets 192.168.1.12 as the IP address of the collector.

2. **(config)# sflow sample 512**

Monitors the traffic every 512 packets.

3. **(config)# sflow additional-http-port 8080**

When URL information is used in the extended data format, configure an additional destination port number 8080 for packets that are determined to be HTTP packets.

4. **(config)# interface gigabitethernet 1/4**

Switches to the configuration command mode for port 1/4.

5. **(config-if)# sflow forward ingress**

Activates the flow sample creation functionality for the received packets and the counter sample creation functionality for the packets sent and received on port 1/4.

##### **Notes**

Even after this parameter has been configured, destination port number 80 is valid for HTTP packets.

## 10.3 Operation

### 10.3.1 List of operation commands

The following table describes the operation commands for sFlow statistics.

Table 10-17: List of operation commands

Command name	Description
show sflow	Shows the configuration conditions and operating status of the sFlow statistics functionality.
clear sflow statistics	Clears statistics managed by sFlow statistics.
restart sflow	Restarts the flow statistics program.
dump sflow	Outputs a file containing debug information collected by the flow statistics program.

### 10.3.2 Checking communication with collectors

When you configure the sFlow statistics to send packets to a collector on the Device, verify the following.

#### (1) Connection with the collector

Execute the `ping` command with the IP address of the collector specified to make sure that the IP communication from the Device to the collector is possible. If the communication is not possible, see the manual *Troubleshooting Guide*.

#### (2) sFlow packet communication

On the collector side, make sure that sFlow packets are received.

For the action to be taken if packets are not being received, see the manual *Troubleshooting Guide*.

### 10.3.3 Checking the sFlow statistics during operation

When you use the sFlow statistics on the Device, you must check the following during operation.

#### (1) Number of discarded sFlow packets

Execute the `show sflow` command to display the sFlow statistics. In these statistics, check the number of packets that are discarded. If the number of discarded packets has increased, adjust the sampling interval so that the packets to be discarded do not increase.

Figure 10-11: Result of executing the show sflow command

```
> show sflow
Date 20XX/07/19 12:00:00 UTC
sFlow service status: enable
Elapsed time from sFlow statistics clearance : 8:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate : 60 seconds
  Received sFlow samples: 37269  Dropped sFlow samples: 2093          <-1
  Exported sFlow samples: 37269  Non-exported sFlow samples      :      0
sFlow collector data :
  Collector IP address: 192.168.1.19  UDP:6343  Source IP address: 192.168.1.1
  Send FlowSample UDP packets : 12077  Send failed packets:      0
  Send CounterSample UDP packets: 621  Send failed packets:      0
  Collector IP address: 192.168.1.20  UDP:65535  Source IP address: 192.168.1.1
  Send FlowSample UDP packets : 12077  Send failed packets:      0
  Send CounterSample UDP packets: 621  Send failed packets:      0
sFlow sampling data :
  Configured rate(actual rate) : 1 per 2048 packets(1 per 2048 packets)
```

Configured sFlow ingress ports: 1/2-4

1. Check the value in `Dropped sFlow samples` and if the number of discarded packets increases, adjust the sampling interval settings.

### 10.3.4 Adjusting the sampling interval for sFlow statistics

When the sFlow statistics functionality is used on the Device, the sampling interval can be adjusted as explained below.

#### (1) Adjusting the line speed

Check the amount of packet flow (packet/s) in all the ports with sFlow statistics functionality enabled, by using the `show interfaces` command, and then sum up the values in `Input rate`. The value calculated by dividing the total value by 1000 gives a sampling interval. Set the sampling interval by using this value, and then use the `show sflow` command to check whether the number of packets to be discarded increases.

The following example shows a sampling interval that can be used as a guideline for retrieving receive packets on ports 1/4 and 3/1.

*Figure 10-12: Result of executing the show interfaces command*

```
> show interfaces gigabitethernet 1/4
Date 20XX/07/19 12:00:00 UTC
NIF1 : active 12-port 10BASE-T/100BASE-TX/1000BASE-T retry:0
      Average:700Mbps/24Gbps Peak:750Mbps at 08:10:30
Port4: active up 1000BASE-T full(auto) 0012.e240.0a04
      Time-since-last-status-change:10:30:30
      Bandwidth:1000000kbps Average out:350Mbps Average in:350Mbps
      Peak out:380Mbps at 08:10:30 Peak in:370Mbps at 08:10:30
      Output rate:290.0Mbps 70.8kpps
      Input rate:290.0Mbps 70.8kpps
      Flow control send :off
      Flow control receive:off
      TPID:8100
      :

> show interfaces gigabitethernet 3/1
Date 20XX/07/19 12:01:00 UTC
NIF3 : active 12-port 10BASE-T/100BASE-TX/1000BASE-T retry:0
      Average:700Mbps/24Gbps Peak:750Mbps at 08:10:30
Port1: active up 1000BASE-T full(auto) 0012.e220.ec31
      Time-since-last-status-change:1:47:47
      Bandwidth:1000000kbps Average out:5Mbps Average in:605Mbps
      Peak out:5Mbps at 15:44:36 Peak in:705Mbps at 15:44:18
      Output rate:4893.5kbps 512pps
      Input rate:634.0Mbps 310.0kpps
      Flow control send :off
      Flow control receive:off
      TPID:8100
      :
```

Sampling interval to be used as a guideline:

$$\begin{aligned}
 &= \text{total-PPS-value-of-the-ports-on-which-the-sFlow-statistics-functionality-is-enabled} / 1000 \\
 &= (70.8 \text{ kpps} + 310.0 \text{ kpps}) / 1000 \\
 &= 380.8^{\#}
 \end{aligned}$$

$\#$ : When the sampling interval is set to 381, the operation is actually performed with the sampling interval set to 512. For details about sampling intervals, see *sflow sample* in the manual *Configuration Command Reference Vol. 2 For Version 12.1*.



## Chapter

---

# 11. CFM

---

CFM (Connectivity Fault Management) verifies the connectivity at the Layer 2 level and confirms routes; in other words, it is functionality for managing and maintaining wide-area Ethernet networks.

This chapter describes CFM and how to use it.

- 11.1 Description
- 11.2 Configuration
- 11.3 Operation

## 11.1 Description

### 11.1.1 Overview

In addition to enterprise LANs, Ethernet is also starting to be used for wide area networks. As a result, maintenance and management functionality on a par with SONET and ATM is required for Ethernet.

The CFM functionality uses the following three main types of functionality to maintain and manage Layer 2 networks:

1. Continuity check

This functionality always monitors whether information is delivered correctly to the destination (accessibility and continuity) between management points.

2. Loopback

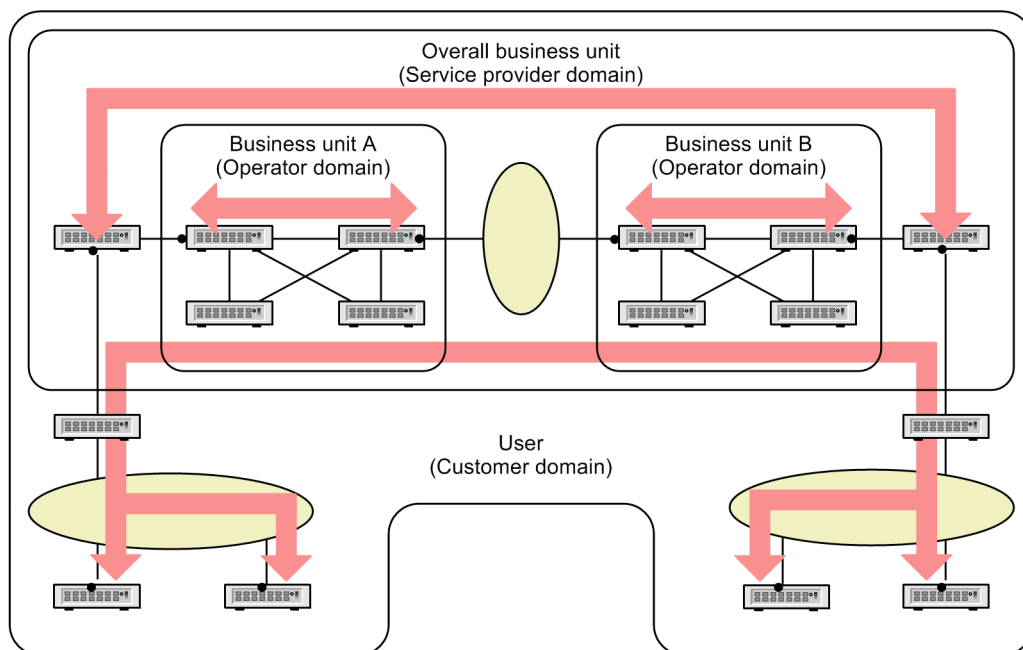
After a failure is detected, the loopback functionality identifies the area affected by the failure on the route (loopback test).

3. Linktrace

After a failure is detected, the linktrace functionality verifies the route to a management point (route searching within a Layer 2 network).

The following figure shows a configuration example of CFM.

Figure 11-1: Example of a CFM configuration



Legend: • : Management point

← : Verify connectivity

#### (1) CFM functionality

There are two standards for CFM: IEEE 802.1ag and ITU-T Y.1731. ITU-T Y.1731 includes the functionality equivalent to IEEE 802.1ag and some other functionality unique to it. The Device supports the functionality for both of the standards. The following tables describe the functionality

for each standard.

*Table 11-1: IEEE 802.1ag CFM functionality*

Function name	Description	Supported
Continuity check (CC)	Continuously monitors accessibility between management points.	Y
Loopback	Loopback test. Executes ping-equivalent functionality in Layer 2.	Y
Linktrace	Route search. Executes traceroute-equivalent functionality in Layer 2.	Y
RDI	Notifies the other management points of the detected failure (part of CC).	Y

Legend: Y: Supported

*Table 11-2: ITU-T Y.1731 CFM functionality*

Function name	Description	Supported
ETH-CC (CC)	Continuously monitors accessibility between management points.	Y
ETH-LB (Loopback)	Loopback test. Executes ping-equivalent functionality in Layer 2.	Y
ETH-LT (Linktrace)	Route search. Executes traceroute-equivalent functionality in Layer 2.	Y
ETH-RDI (RDI)	Notifies the other management points of the detected failure.	Y
ETH-AIS	Notifies the higher domain of the failure in lower domain.	O
ETH-LCK	Controls failure detection for the test such as ETH-Test.	O
ETH-Test	Detailed measurement of frame loss or bit error and so on	N
ETH-APS	Fast protection switching (50 msec) in case of failure	N
ETH-MCC	Signal channel for maintenance	N
ETH-EXP	For experiment	N
ETH-VSP	For implementation of vendor-specific functionality	N
ETH-LM	Frame loss measurement	N
ETH-DM	Transmission delay measurement	N
ETH-CSF	Client signal failure	N
ETH-SLM	Synthetic frame loss measurement	N

Legend: Y: Supported, O: Supported only at the receiving side, N: Not supported

## **(2) CFM configuration**

The table below describes the elements configuring CFM.

Table 11-3: Elements configuring IEEE 802.1ag CFM

Element	Description
Domain (Maintenance Domain)	For management purposes, a group on the network to which CFM is applied
Domain level	Level of domains
MA (Maintenance Association)	A group used to subdivide a domain for management purposes
MAID (Maintenance Association Identifier)	Identifier for MA An identifier consists of a domain name, MA number, and MA name.
MEP (Maintenance association End Point)	A management end point Set a MEP on the port at the domain boundary for each MA. In addition, the port is used to execute the CFM functionality. There are two types of MEPs: Down MEPs and Up MEPs.
Down MEP	MEP that sends and receives CFM PDUs directly.
Up MEP	MEP that sends and receives CFM PDUs indirectly through other ports by using the L2 forward functionality.
MIP (Maintenance domain Intermediate Point)	A management intermediate point. This management point is located inside a domain.
MP (Maintenance Point)	A management point and the generic name used for a MEP or a MIP

Table 11-4: Elements configuring ITU-T Y.1731 CFM

Element	Description
MEG (Maintenance Entity Group)	A group of management points
MEG level	Level of MEG
MEG ID	Identifier for MEG An identifier configured according to the MEG name
MEP (Maintenance entity group End Point)	A management end point To be set for the port at the management boundary for each MEG. In addition, the port is used to execute the CFM functionality. There are two types of MEPs: Down MEPs and Up MEPs.
Down MEP	MEP that sends and receives CFM PDUs directly.
Up MEP	MEP that sends and receives CFM PDUs indirectly through other ports by using the L2 forward functionality.
MIP (Maintenance entity group Intermediate Point)	A management intermediate point. This management point is located inside a MEG.
Server MEP	The MEP required for the operation of ETH-AIS. Automatically configured when a MEP is set.

The following correspondence table describes the terms for IEEE 802.1ag and ITU-T Y.1731.

*Table 11-5: Correspondence between the terms for IEEE 802.1ag and ITU-T Y.1731*

Terms in IEEE 802.1ag	Terms in ITU-T Y.1731	Terms used in this manual	Remarks
Domains	--	Domains	In this manual, the MEGs in the same MEG level are referred to as a domain.
Domain level	MEG level	Level	--
MA	MEG	MA	In this manual, the term MA is used if the described item is common to IEEE 802.1ag and ITU-T Y.1731. If a distinction is needed, a term such as IEEE 802.1ag MA is used
MAID	MEG ID	MAID	In this manual, the term MA ID is used if the described item is common to IEEE 802.1ag and ITU-T Y.1731. If a distinction is needed, a term such as IEEE 802.1ag MA ID is used.
MEP	MEP	MEP	--
Down MEP	Down MEP	Down MEP	--
Up MEP	Up MEP	Up MEP	--
MIP	MIP	MIP	--
MP	--	MP	In this manual, MP is used as a generic term for MEP and MIP.
--	Server MEP	Server MEP	Server MEP is the functionality unique to ITU-T Y.1731.

Legend: --: Not applicable

### (3) Support status

The following table describes the support status for CFM configuration elements on the Device.

*Table 11-6: Support status for CFM configuration elements*

Terms used in this manual	Supported
Domains	Y
Level	Y
MA	Y
MAID	Y
Down MEP	Y
Up MEP	N
MIP	N
Server MEP	Y

Legend: Y: Supported, N: Not supported

### 11.1.2 CFM configuration elements

#### (1) Domains

CFM manages a network hierarchically on a domain-by-domain basis, and maintains and manages the network by sending and receiving CFM PDUs within a domain. Domains are classified into eight levels from 0 to 7, with larger values indicating a higher level.

A higher-level domain means that CFM PDUs of lower-level domains are discarded. A lower-level domain forwards the CFM PDUs of higher-level domains without processing them. Accordingly, the CFM PDUs of lower-level domains are not forwarded to a higher-level domain and thus each domain can be maintained and managed independently.

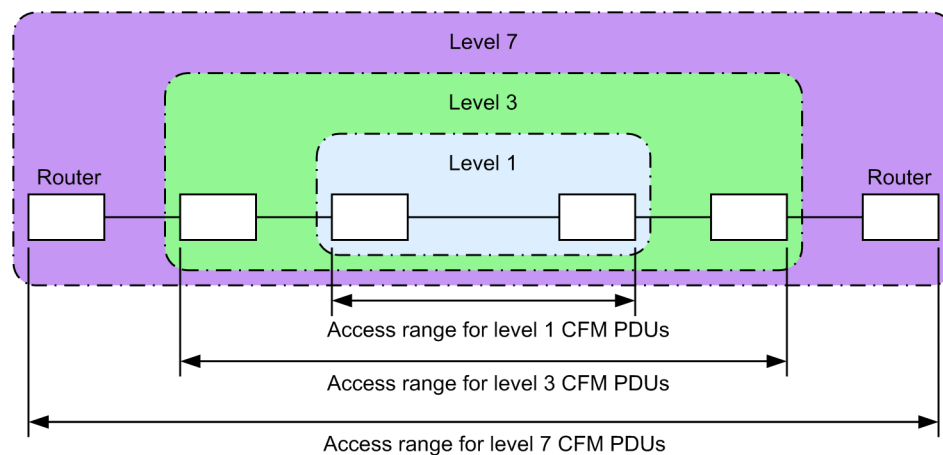
Standards stipulate that levels are to be used according to categories. The following table describes the levels assigned to each category.

*Table 11-7: Levels assigned to the categories*

Level	Category
7	Customer (user)
6	
5	
4	Service provider (overall business unit)
3	
2	
1	Operator (business unit)
0	

Domains can be set hierarchically. To hierarchically configure domains, place a lower level inside and higher level outside. The following figure shows a configuration example of hierarchical domains.

*Figure 11-2: Example configuration of hierarchical domains*



#### (2) MA

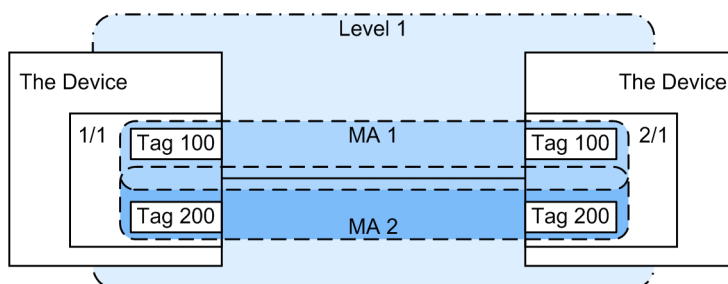
An MA is used to manage a domain by subdividing it. A domain must have at least one MA.

Because CFM can be used in an MA, setting MAs can divide the management range up even further.

MAs are identified by an MA ID. Accordingly, for the devices used in the same MA, the same MA ID must be specified.

The following figure shows an example of the scope of MA management.

Figure 11-3: Example of MA management scope



### (3) MEP

A MEP is a management point on a domain boundary, and is specified for an MA. A MEP is identified by a MEP ID, which is unique within the MA.

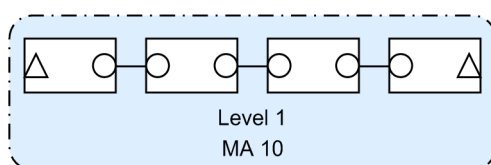
The CFM functionality is executed at a MEP. When CFM PDUs are sent and received between MEPs (that is, at domain boundaries), CFM is able to check the connectivity of the applicable network.

There are two types of MEPs:

#### ■ Up MEP

An Up MEP uses L2 forward functionality to send and receive CFM PDUs. The following figure shows a configuration example of Up MEPs.

Figure 11-4: Configuration example of Up MEPs

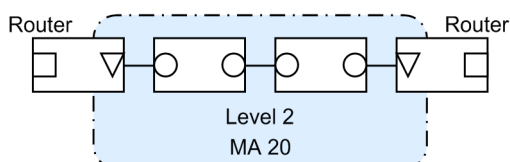


Legend:  $\triangle$ : Up MEP    $\circ$ : MIP

#### ■ Down MEP

The Down MEP sends and receives CFM PDUs itself. The following figure shows a configuration example of Down MEPs.

Figure 11-5: Configuration example of Down MEPs



Legend:  $\nabla$ : Down MEP    $\circ$ : MIP    $\square$ : Port (other than MEP and MIP)

The following figures show how CFM PDUs are sent from the Down MEP and the Up MEP and received at the Down MEP and the Up MEP.

Figure 11-6: Sending CFM PDUs from a Down MEP or an Up MEP

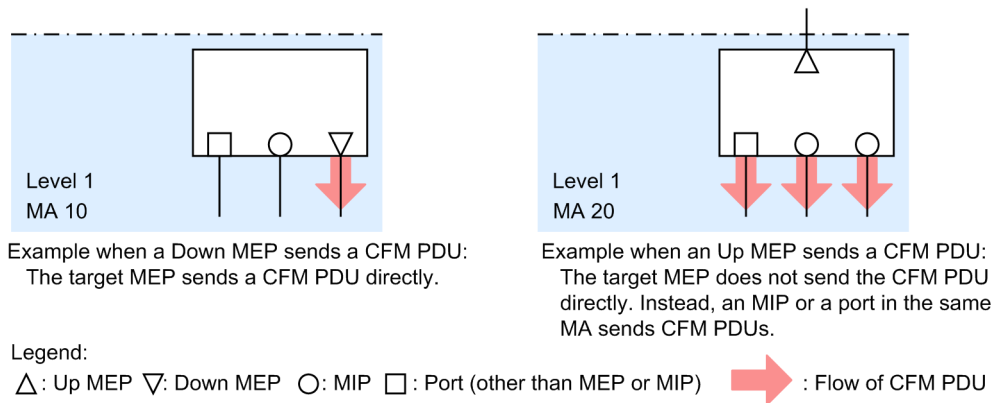
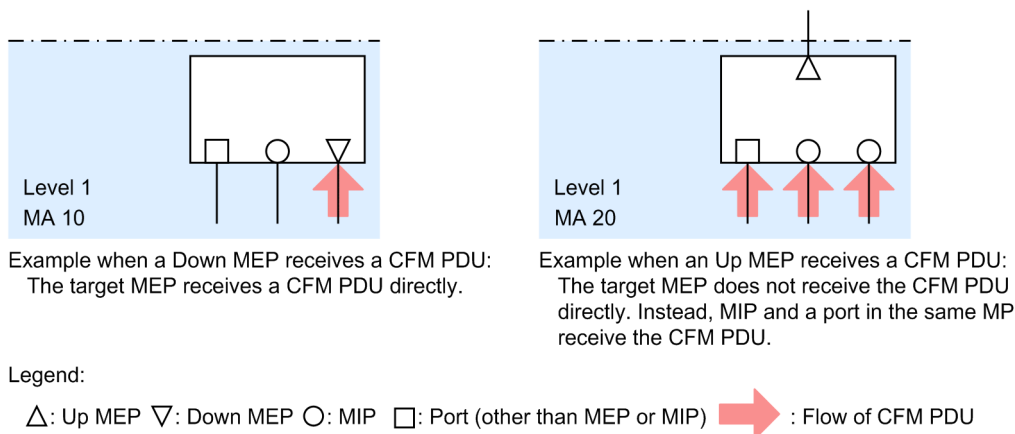
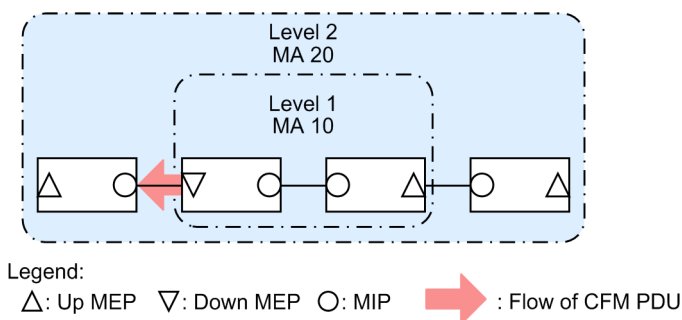


Figure 11-7: Receiving CFM PDUs at a Down MEP or an Up MEP



Set the Down MEP and the Up MEP at the correct locations. For example, a Down MEP must be set at the inner side of an MA. If you place a Down MEP at the outer side of an MA, CFM does not function correctly because CFM PDUs are sent outside the MA. The following figure shows an example of a Down MEP that is set incorrectly.

Figure 11-8: Example of a Down MEP that is set incorrectly



If you place the Down MEP at the outer side of MA 10, CFM does not function correctly because CFM PDUs are sent outside MA 10 (outside level 1).

#### (4) MIP

An MIP is a management point set inside a domain, and is specified for each domain (and is shared by all MAs inside a domain). For a hierarchical configuration, set a MIP at the point where a higher-level domain and a lower-level domain overlap. In addition, because MIPs respond to the loopback functionality and the linktrace functionality, set a MIP inside a domain at the point where



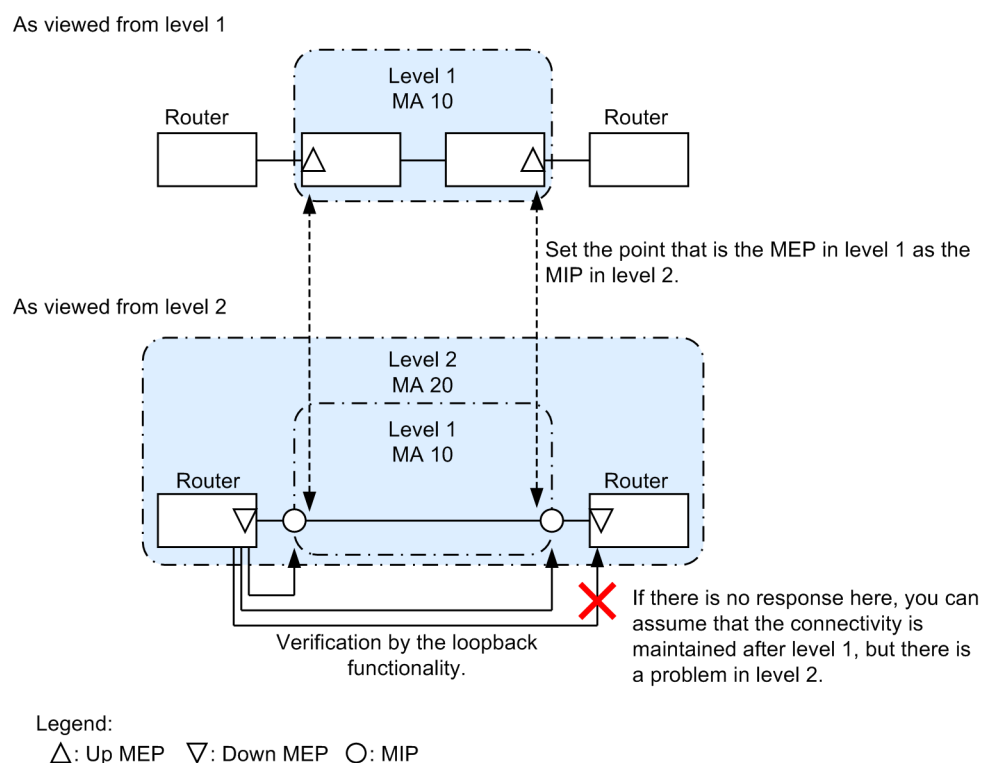
you want maintenance and management to occur.

**(a) When setting a MIP at the point where domains overlap**

If you set a MIP at the point where domains overlap, you can manage these domains in a state in which a higher domain recognizes a lower domain, but in which the higher domain is unaware of the configuration of the lower domain.

The following figure shows an example of a hierarchical structure configured by levels 1 and 2.

*Figure 11-9: Example of a hierarchical structure configured by levels 1 and 2*



When designing level 2, specify a port set as a MEP in an MA of level 1 as a MIP for level 2. By doing so, you can manage level 2 without being aware of level 1 during operation, even if level 2 recognizes the level 1's range.

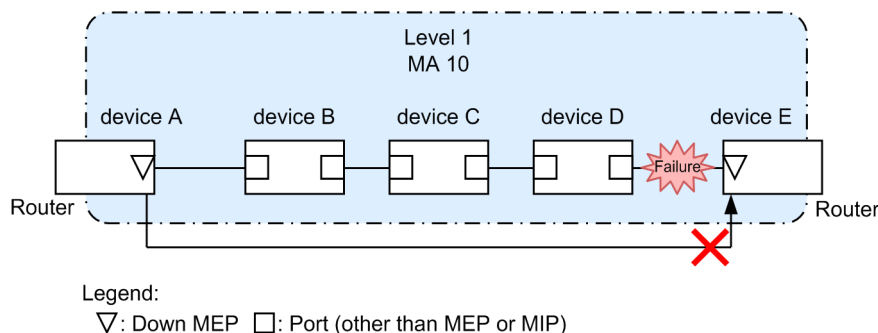
If a failure occurs, you can narrow down the scope of the investigation because you are able to isolate the cause of the failure to level 1 or level 2.

**(b) When setting a MIP at the point where you want maintenance and management to occur**

The more MIPs you specify in a domain, the more precisely you can maintain and manage the domain.

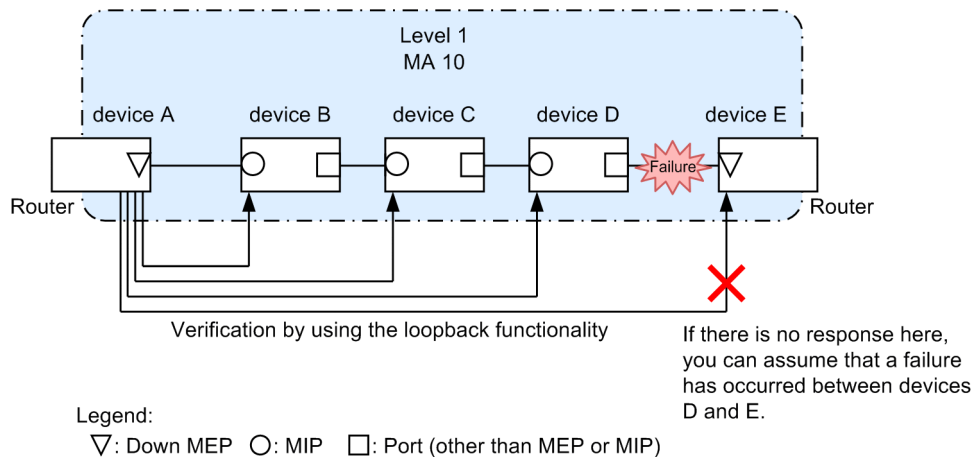
The figure below shows an example configuration where no MIPs are set in a domain. In this example, if a network failure occurs, you can confirm that the MEP of device A cannot communicate with the MEP of device E, but you cannot identify the point at which the failure occurred.

Figure 11-10: MIPEXample configuration in which no MIPs are set in a domain



The figure below shows an example configuration in which MIPs are set in a domain. In this example, you can determine the point at which a failure occurs because the MIPs in the domain make it possible for each device to respond to the loopback or linktrace functionality.

Figure 11-11: Example configuration where MIPs are set in a domain



### (5) Server MEP

A server MEP is a virtual MEP that is needed when ETH-AIS is used. When the server MEP receives an AIS frame, it sends the AIS frame to a higher-level MEP.

For details about ETH-AIS, see 11.1.7 *ETH-AIS*.

## 11.1.3 Designing domains

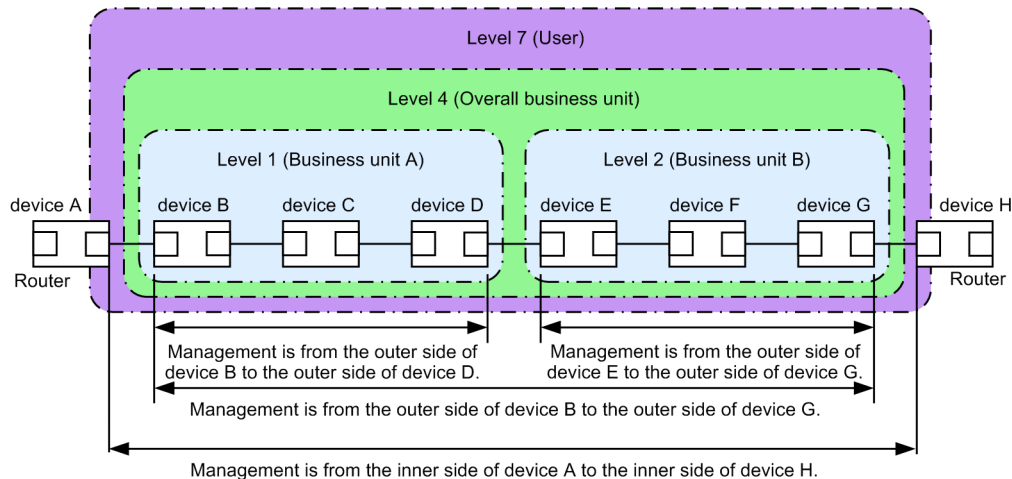
To use the CFM functionality, design the domains first. Then design the domain configurations and their hierarchies, and finally design the details of each domain.

When you design a domain, you must configure the level, MAs, MEPs, and MIPs.

### (1) Designing the domain configuration and its hierarchy

Set an MA port (for which the MA is the boundary between domains) as a MEP and set a port that overlaps with the lower domain as a MIP. The procedure for designing the domain configuration and the hierarchy is described below according to the configuration example shown in the following figure.

Figure 11-12: Configuration example



Legend: □: Port

Design the domains as units, such as business unit A, business unit B, the overall business unit, and user, and then specify the level appropriate for the category. Also, the following items are assumed:

- Business unit A, business unit B, and the overall business unit manage connectivity, including the ports to be provided to users, in order to ensure the availability of lines that need to be provided to users.
- Users manage the connectivity of the line provided by a business unit in order to monitor the availability of that line.

Design a domain from the lowest level up as described below.

#### • Configuring levels 1 and 2

1. Set MA 10 for level 1.

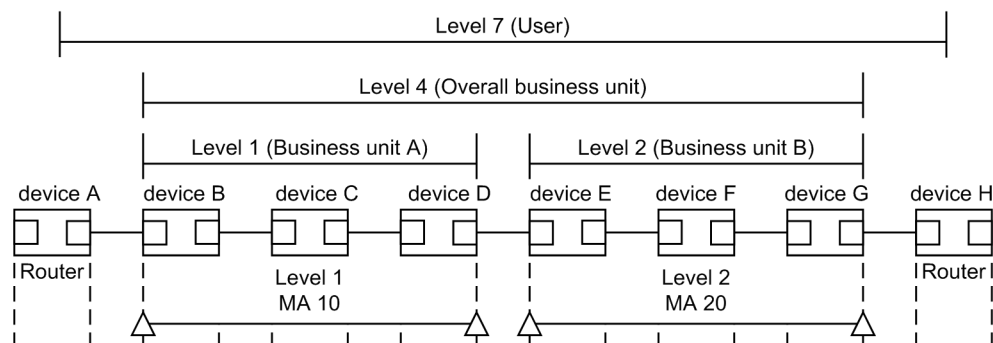
In this example, one domain is managed by one MA. If you want to manage the domain more precisely by subdividing it into VLAN groups, set an MA for each management unit.

2. Set an MA port as a MEP on devices B and D, which are on the domain boundary.

The business unit configures the Up MEPs in order to manage the connectivity, including the ports to be provided to users.

3. Set an MA for level 2 as well, and configure an Up MEP on devices E and G.

Figure 11-13: Configuring levels 1 and 2



Legend:

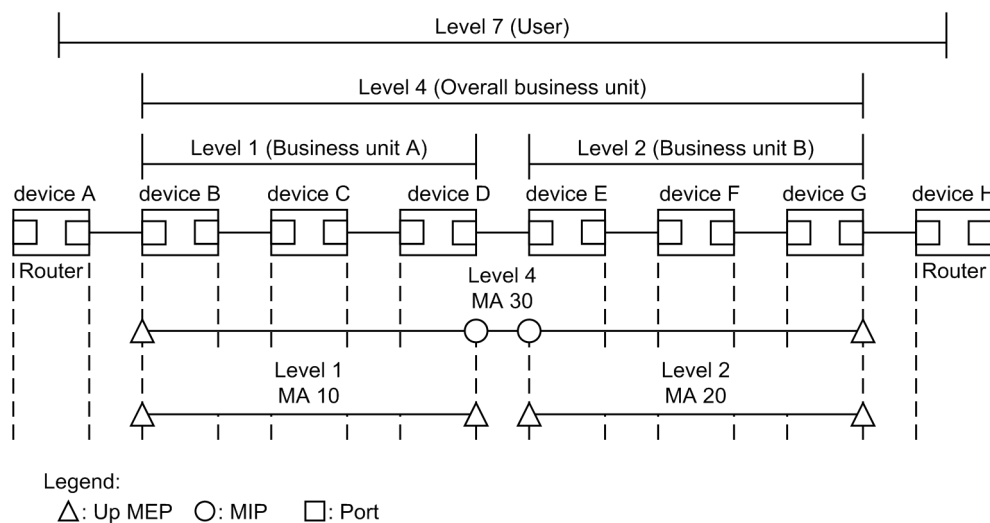
Δ: Up MEP □: Port

- **Configuring level 4**

1. Set MA 30 for level 4.
2. Set an MA port as a MEP on devices B and G, which are on the level 4 boundary.  
The business unit configures the Up MEPs in order to manage the connectivity, including the ports to be provided to users.
3. Because level 4 contains levels 1 and 2, configure MIPs on devices D and E, which are the relay points of each level.

If you set a MEP of a lower domain as a MIP in a higher domain, you can identify the scope of investigation more easily because you can use the loopback or linktrace functionality to determine if the problem has occurred in the domain you manage or in a lower-level domain.

Figure 11-14: Configuring level 4

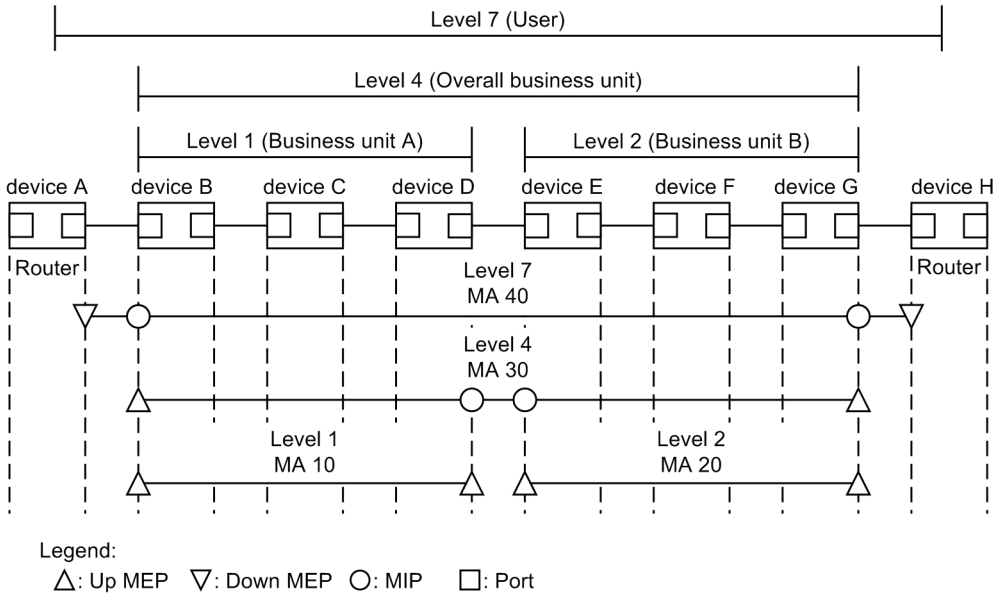


- **Configuring level 7**

1. Set MA 40 for level 7.
2. Set an MA port as a MEP on devices A and H, which are on the level 7 boundary.  
In order to manage the connectivity of the lines provided by business units, users configure the Down MEP.
3. Because level 7 contains level 4, configure MIPs on devices B and G, which are the relay points.

Because levels 1 and 2 are specified as relay points of level 4, you do not need to configure levels 1 and 2 in level 7.

Figure 11-15: Configuring level 7



(2) Detailed design of each domain

For the detailed design, configure, as MIPs, the points to which you want to apply the loopback functionality and the linktrace functionality.

The following figures show configuration examples before and after MIPs are set.

Figure 11-16: Example configuration before MIPs are set

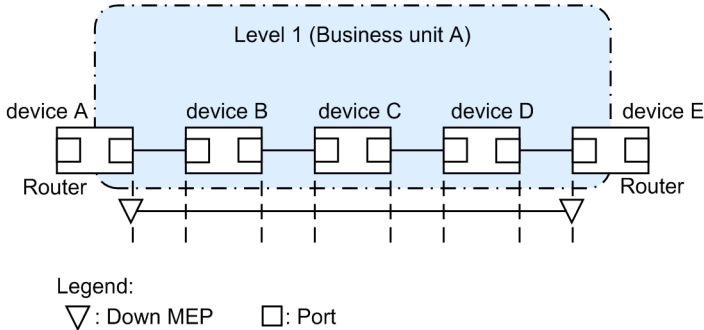
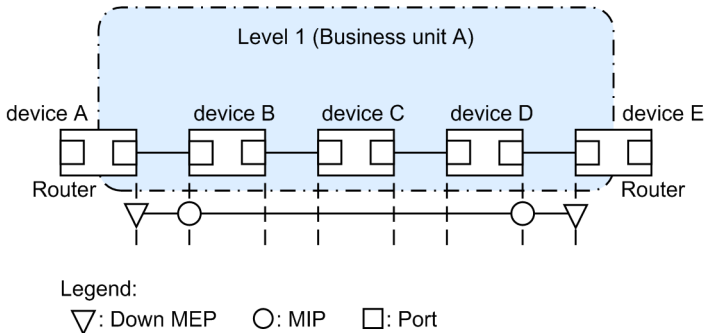


Figure 11-17: Example configuration after MIPs are set



Inside the domain, specify, as MIPs, the ports to be configured as the destination of the loopback functionality and the linktrace functionality. In this example, MIPs are set on devices B and D. With this configuration, you can perform loopback and linktrace for the MIPs on devices B and D. In addition, routing information of the linktrace functionality is returned as a response.

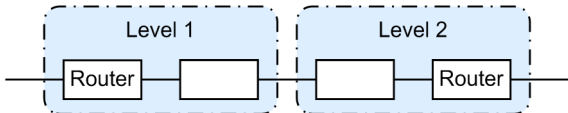
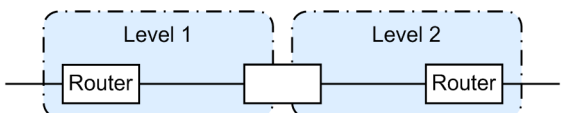
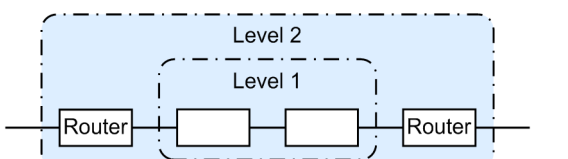
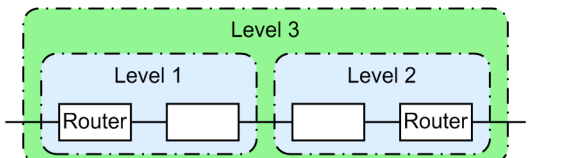
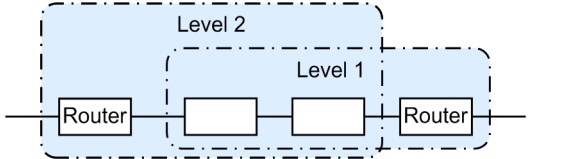
You cannot specify device C as the destination for loopback and linktrace because no MIPs are configured on device C. In addition, because device C does not respond to the linktrace functionality, information about device C is not contained in routing information.

### (3) Domain configuration examples

Domains can be configured hierarchically. The inner part of the hierarchy must be configured as lower-level domains and the outer part as higher-level domains.

The following table describes configuration examples and states whether they are possible or not.

Table 11-8: Example of possible and impossible domain configurations

Configuration status	Configuration example	Configurable
Neighboring domains		Yes
Touching domains		Yes
Nested domains		Yes
Combination of neighboring domains and nested domains		Yes
Overlapping domains		No

## 11.1.4 Continuity check

The continuity check (CC) is functionality that continuously monitors the connectivity between MEPs. All MEPs in an MA send and receive CCMs (continuity check messages, a type of CFM PDU) mutually and learn the MEPs in the MA. What the MEPs learn is used for the loopback functionality and the linktrace functionality.

### (1) Failures detected by the CC functionality

If a device on which the CC functionality is used does not receive CCMs or a port in the MA of the applicable device cannot communicate, a failure is determined to have occurred. When this happens, a CCM with a failure detection flag is sent to notify MEPs in the MA of the failure.

The table below describes the failures detectable by the CC functionality of IEEE 802.1ag. There are five such failure levels for the failures detected by the CC functionality of IEEE 802.1ag. The Device is initially configured to detect level 2 and higher failures.

Table 11-9: Failures detected by the CC functionality of IEEE 802.1ag

Failure level	Failure description	Initial state
5	A domain and the MA received different CCMs.	Detected
4	A CCM with an incorrect MEP ID or an incorrect sending interval was received.	
3	CCMs are no longer received.	
2	A port on the applicable device has entered a state in which it is unable to communicate.	
1	A CCM reporting failure detection was received. Remote Defect Indication	Not detected

When the failure recovery monitoring time after the failure recovery trigger point has elapsed, it is determined that recovery from the failure has succeeded.

Table 11-10: Failure recovery trigger point and failure recovery monitoring time in IEEE 802.1ag

Failure level	Failure recovery trigger point	Failure recovery monitoring time
5	A domain and an MA no longer receive different CCMs.	<i>sending-interval-of-the-received-CCMs</i> x 3.5
4	A CCM with an incorrect MEP ID or an incorrect sending interval is no longer received.	
3	A CCM is received again.	Immediately after reception of the CCM
2	A CCM indicating that the port on the applicable device can now communicate.	
1	A CCM indicating no failure is detected is received.	

The following describes the failures to be detected by the CC functionality of ITU-T Y.1731. Note that there are no failure levels for the failures detected by CC of ITU-T Y.1731.

- A CCM with an invalid MA ID is received.
- A CCM with an invalid level is received.
- A CCM with an incorrect MEP ID is received.
- A CCM with a different CoS value is received.
- A CCM with an incorrect sending interval is received.
- CCMs are no longer received.

When the failure recovery monitoring time after the failure recovery trigger point has elapsed, it is determined that recovery from the failure has succeeded.

Table 11-11: Failure recovery trigger point and failure recovery monitoring time in ITU-T Y.1731

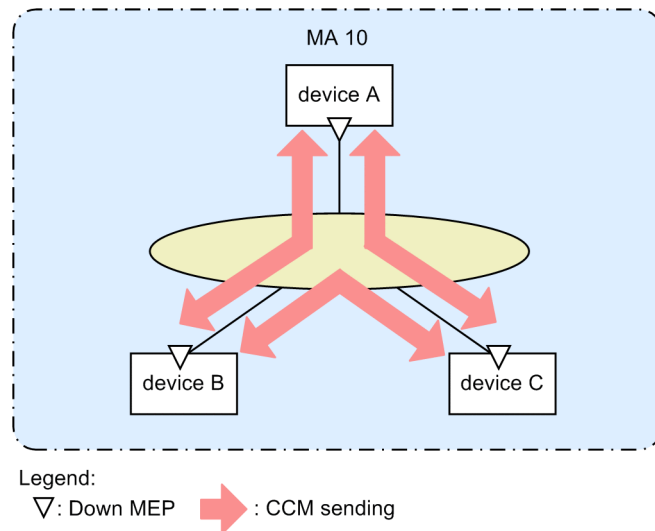
Failure recovery trigger point	Failure recovery monitoring time
CCMs with a different MA ID are no longer received.	<i>sending-interval-of-the-received-CCMs</i> × 3.5
CCMs with an invalid level are no longer received.	
CCMs with an incorrect MEP ID are no longer received.	
CCMs with a different CoS value are no longer received.	
CCMs with an incorrect sending interval are no longer received.	
A CCM is received again.	Immediately after reception of the CCM

## (2) Behavior of the CC functionality

CC functionality behavior will be described using device B in the following figures as an example.

Each MEP multicasts a CCM regularly inside the MA. Because CCMs are received from each MEP regularly, connectivity is always monitored.

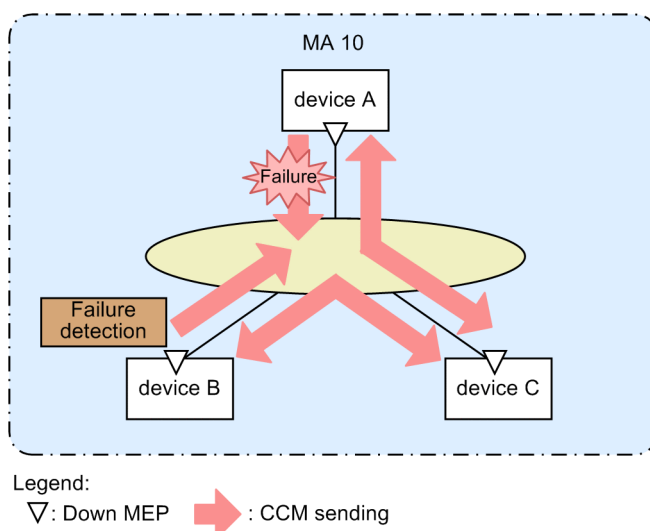
Figure 11-18: Continuous monitoring of connectivity using CC



If a CCM from device A cannot be delivered to device B because of a device failure or a network failure, device B determines that the state is a network failure between devices A and B.

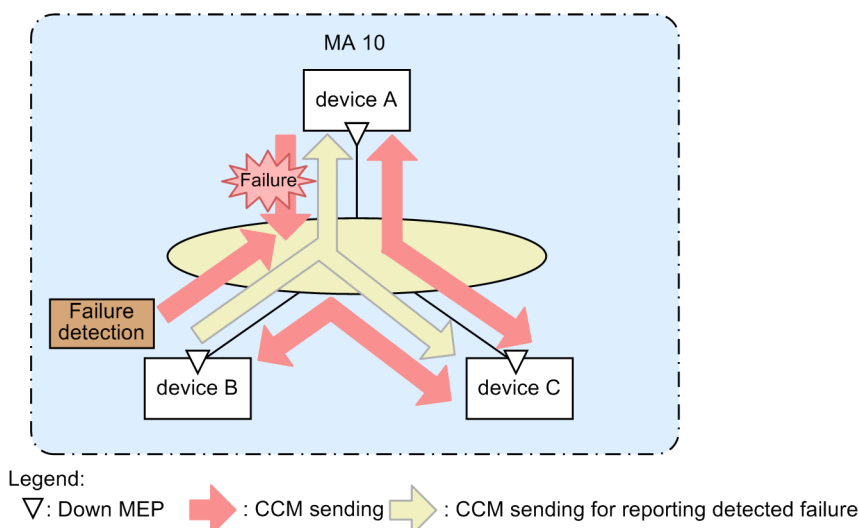


Figure 11-19: Detecting a failure with CC



When device B detects a failure, device B notifies all MEPs in the MA that a failure has been detected.

Figure 11-20: Notifying all MEPs of the failure



The MEPs that received the CCM indicating a detected failure acknowledge that a failure has occurred somewhere in the MA. If loopback and linktrace are performed on each device, the devices can determine the route inside the MA on which the failure occurred.

### 11.1.5 Loopback

The loopback functionality can be used at the Layer 2 level, and is equivalent to pinging. The loopback functionality verifies the connectivity between MEPs or between a MEP and a MIP in the same MA.

CC verifies the connectivity between MEPs. The loopback functionality can additionally verify the connectivity between a MEP and a MIP, with the result that it can check the connectivity in an MA in greater detail.

Connectivity is verified by sending a loopback message (a kind of CFM PDU) from the MEP to the destination and confirming that the destination responds to the message.

The MIP or MEP responds directly to the loopback functionality. If, for example, multiple MIPs

are configured on a device, connectivity can be verified for each MIP.

The following figures show examples of executing the loopback for MIPs and MEPs.

Figure 11-21: Execution of loopback to MIP

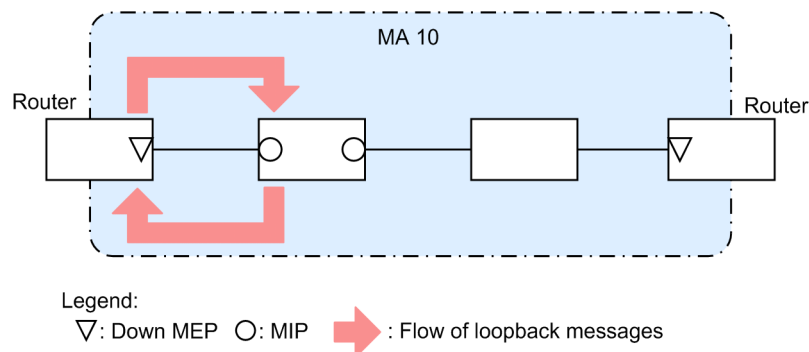
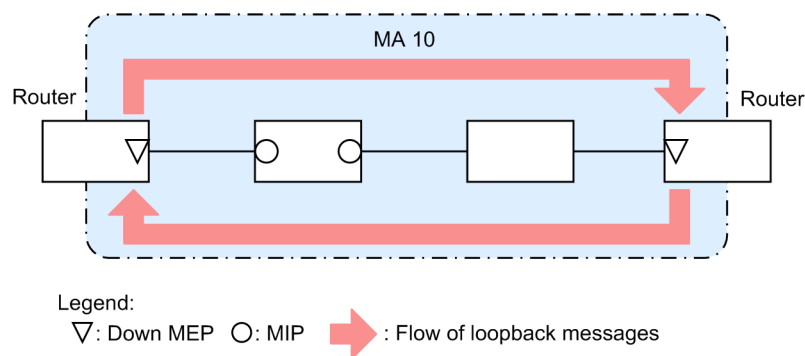


Figure 11-22: Execution of loopback to MEP



Because the loopback functionality uses what CC learns, CC must be started beforehand. If you configure a MIP on the destination device, you must note the MAC address of the port used as the MIP beforehand.

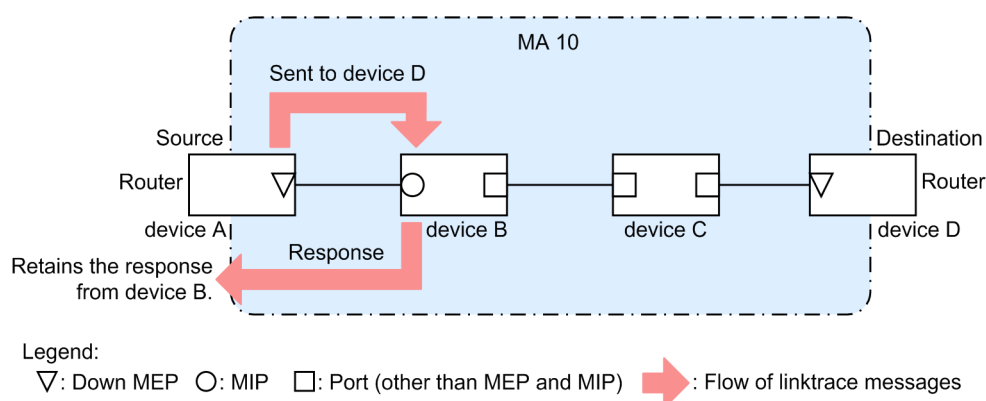
### 11.1.6 Linktrace

The linktrace functionality can be used at the Layer 2 level, and is equivalent to traceroute. The linktrace functionality collects information about devices that pass traffic between MEPs or between a MEP and a MIP of the same MA, and outputs routing information.

The linktrace functionality sends a linktrace message (a kind of CFM PDU) and collects the returned responses as routing information.

The following figure shows an example of sending a linktrace message to a destination.

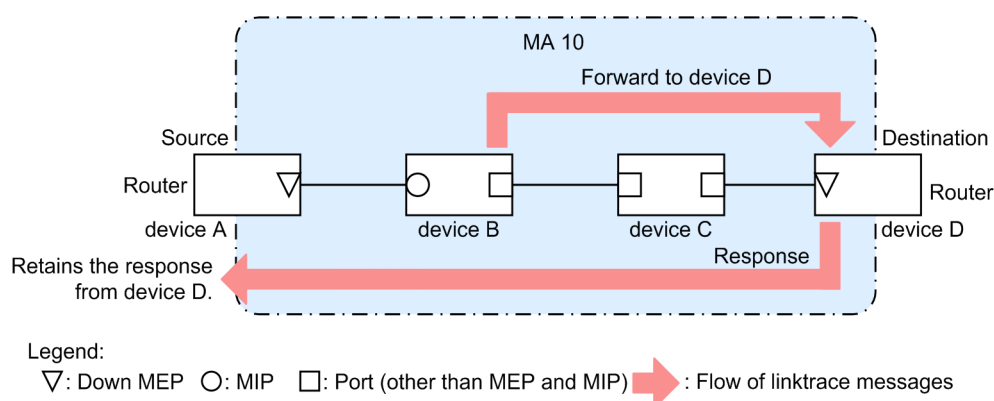
Figure 11-23: Sending a linktrace message to a destination



A linktrace message is forwarded to the destination via MIPs. An MIP sends back information about the port of the local device used to receive the MIP and the ports used to forward the MIP. The device from which the message was sent (the source device) keeps the information sent by the MIPs as routing information.

The following figure shows an example of forwarding a linktrace message to the destination.

Figure 11-24: Forwarding of a linktrace message to a destination



The MIP that sent back the information forwards the linktrace message to the destination. However, device C in the above figure does not send back the information because MEPs or MIPs are not configured on device C. At least one MIP must be configured on a device in order to send back information.

When a linktrace message reaches the MEP or the MIP at the destination, a message containing information about the MEP or MIP at the destination to which the linktrace message was delivered and the port through which the message was received is delivered to the source device.

The source device outputs the information it has retained as routing information that can be used to check the route to the destination.

The linktrace functionality provides information for each device. For example, whether one or multiple MIPs are configured on a device, the linktrace functionality provides information about the port used to receive the message and the port used to forward the message.

Because the linktrace functionality uses what CC learns, CC must be started beforehand. If you configure a MIP on the destination device, you must note the MAC address of the port used as the MIP beforehand.

#### (a) Using the linktrace functionality to isolate failures

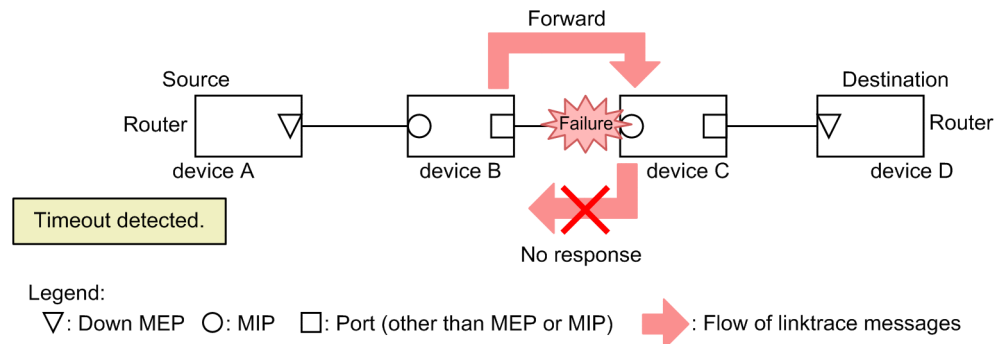
You can use the execution results of the linktrace functionality to isolate the device or port on

which a failure has occurred.

- **When a timeout is detected**

The following figure shows an example of timeout detection by the linktrace functionality.

*Figure 11-25: Example timeout detection by the linktrace functionality*

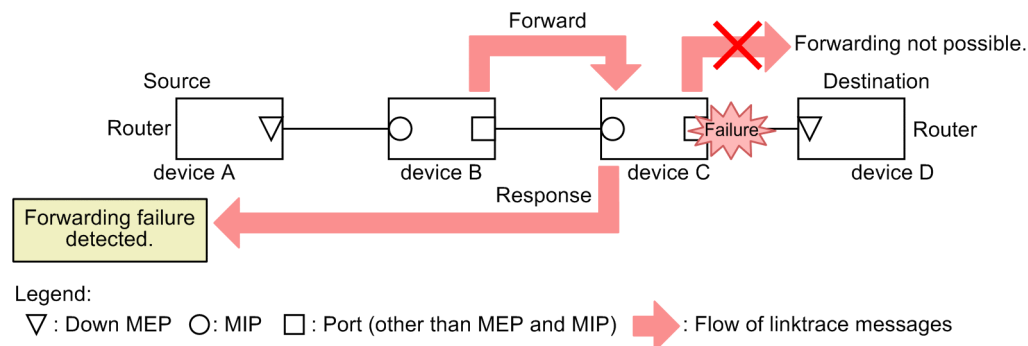


In this example, when device A detects a timeout by using the linktrace functionality, a receiving port on the network might not be able to communicate. A linktrace message is forwarded from device B to device C, but because device C cannot communicate and cannot return a response, a timeout occurs.

- **When a forwarding failure is detected**

The following figure shows an example of a communication failure detected by the linktrace functionality.

*Figure 11-26: Example of detection of a communication failure by the linktrace functionality*



If device A detects a forwarding failure by using the linktrace functionality, a sending port on the network might not be able to communicate. The reason is that a linktrace message cannot be forwarded to devices C and D (destination), and therefore the linktrace functionality returns a message indicating that a sending port cannot communicate with device A.

**(b) Linktrace response**

Linktrace messages are multicast frames.

When forwarding linktrace messages between devices on which CFM is used, see the MEP CCM database to determine the port used to forward linktrace messages.

Devices on which CFM is not used flood linktrace messages. As a result, if there is a device on the network on which CFM is not used, responses are returned from devices that are not on the route to the destination.

### 11.1.7 ETH-AIS

ETH-AIS is functionality to notify higher-level MEPs of a failure detected in a lower level. ETH-AIS is defined in ITU-T Y.1731.

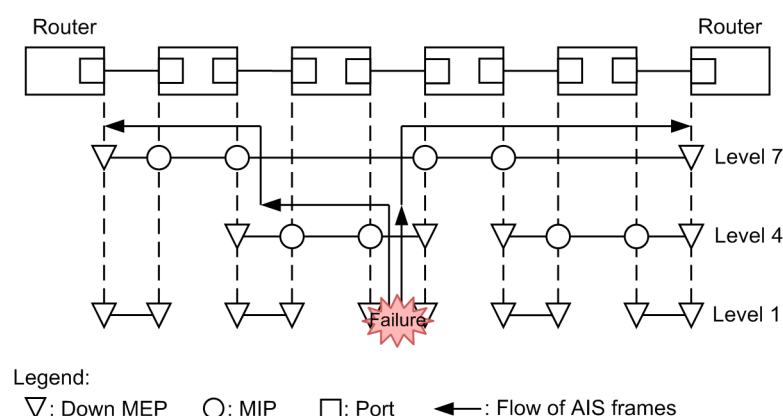
When a failure is detected in a lower level, ETH-AIS sends an AIS frame to higher-level MEPs. The higher-level MEP that receives the AIS frame enters the AIS state and acknowledges that a failure occurred in the lower level.

The MEP in the AIS state suppresses failure detection for unreceived CCMs. Also, it sends an AIS frame to even higher-level MEPs to report the failure to the appropriate higher-level range. By using this functionality, failure detection in a higher level is suppressed in cases where the cause of the failure in the lower level could affect the higher level. For this reason, the determination of the point at which the failure occurred becomes easier.

The Device supports the functionality to suppress failure detection by receiving AIS frames.

The following figure shows the flow of AIS frames.

Figure 11-27: Flow of AIS frames



### 11.1.8 ETH-LCK

ETH-LCK is functionality to stop communication for tests such as ETH-Test and notifies higher-level MEPs of the stop. ETH-AIS is defined in ITU-T Y.1731.

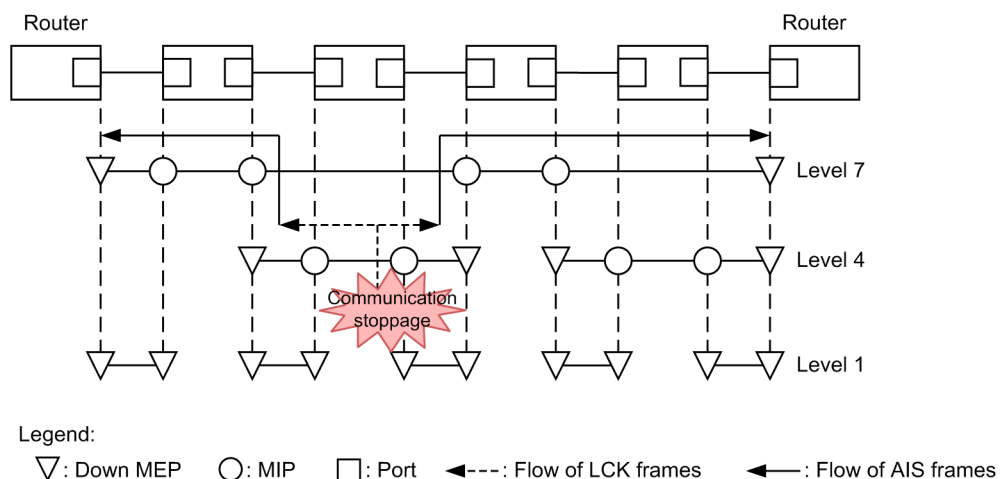
When ETH-LCK stops communication, it sends an LCK frame to higher-level MEPs. The MEP that receives an LCK frame enters the LCK state and acknowledges that the communication is stopped in the lower level.

The MEP in LCK state suppresses the failure detection for the unreceived CCM, and thus suppresses the failure detection caused by tests. Also, it sends the AIS frame to even higher-level MEPs to suppress the failure detection caused by unreceived CCM in the higher level.

The Device supports the functionality to suppress the failure detection by LCK frames.

The following figure shows the flow of LCK frames.

Figure 11-28: Flow of LCK frames



### 11.1.9 Behavior for the port in the communication-blocked state

The following table describes the operation of each functionality when a Down MEP is in a communication-blocked state.

Table 11-12: When a Down MEP is in a communication-blocked state

Functionality	Operation
CC	<ul style="list-style-type: none"> <li>Does not send or receive CCMs.</li> </ul>
Loopback	<ul style="list-style-type: none"> <li>Cannot execute the <code>l2ping</code> operation command.</li> <li>Does not respond to loopback messages sent to the local device.</li> </ul>
Linktrace	<ul style="list-style-type: none"> <li>Cannot execute the <code>l2traceroute</code> operation command.</li> <li>Does not respond to linktrace messages.</li> </ul>
ETH-AIS	<ul style="list-style-type: none"> <li>Does not receive AIS frames.</li> </ul>
ETH-LCK	<ul style="list-style-type: none"> <li>Does not receive LCK frames.</li> </ul>

### 11.1.10 Databases used for CFM

The following table describes the databases used by CFM.

Table 11-13: Databases used for CFM

Database	Description	Command for checking its contents
MEP CCM database	<p>A database maintained by each MEP. Information about MEPs in the same MA. CC uses this database when it monitors pervasive connectivity. The database holds the following information:</p> <ul style="list-style-type: none"> <li>MEP ID</li> <li>MAC addresses corresponding to the MEP ID</li> <li>Information about failures occurring at the applicable MEP.</li> </ul>	<code>show cfm remote-mep</code>

Database	Description	Command for checking its contents
Linktrace database	<p>A database holding the execution results of the linktrace functionality.</p> <p>The database holds the following information:</p> <ul style="list-style-type: none"> <li>• The MEPs and the destinations where the linktrace functionality was executed</li> <li>• TTL</li> <li>• Information about devices that sent back responses</li> <li>• Information about ports on which linktrace messages were received</li> <li>• Information about ports from which linktrace messages were forwarded</li> </ul>	show cfm l2traceroute-db

### (1) MEP CCM database

The MEP CCM database holds information about the types of MEPs that are in the same MA. It also holds information about the failures occurring at the applicable MEPs.

Although you can specify the destination by using the MEP ID for the loopback functionality and the linktrace functionality, the MEP IDs that are not registered in the MEP CCM database cannot be specified. You can use the `show cfm remote-mep operation` command to check if a MEP ID is registered in the database.

An entry in this database is created when a MEP receives a CCM while CC is running.

### (2) Linktrace database

The linktrace database holds the execution results of the linktrace functionality.

You can use the `show cfm l2traceroute-db` operation command to see the results of executing the linktrace functionality in the past.

#### (a) Number of routes that can be held

A device can retain responses for a maximum of 2048 devices.

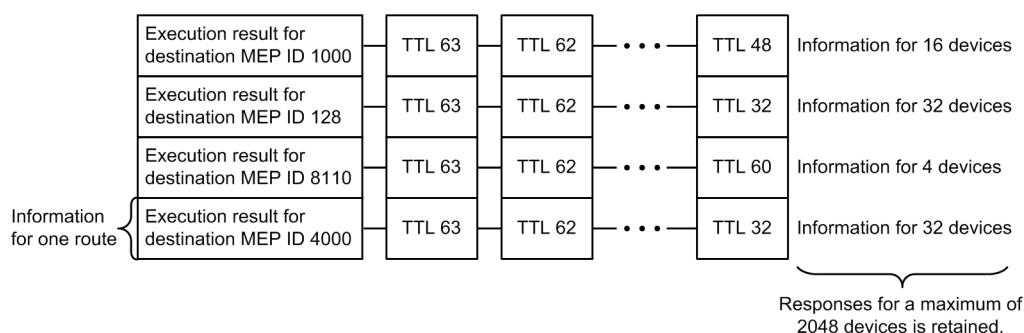
The number of routes that can be retained is determined by the number of devices per route. If you want to retain responses for 256 devices per route, you can have eight routes. If you want to retain responses for 16 devices per route, you can have 128 routes.

If the number of responses exceeds for the number of responses allowed for 2048 devices, information about an old route is deleted, and information about the new route is saved.

When the linktrace functionality is executed at a destination that is registered in the linktrace database, the routing information from the linktrace database to the applicable destination is deleted first, and then the new linktrace response is saved.

The following figures show entries in the linktrace database.

Figure 11-29: Linktrace database



An entry in this database is created when a MEP receives a response while the linktrace functionality is running.

### 11.1.11 Operation when connecting IEEE 802.1ag and ITU-T Y.1731

#### (1) Connecting CC functionality

To connect the CC, the level and MA ID have to match. However, CC functionality provides incompatible MA IDs for IEEE 802.1ag and ITU-T Y.1731 and thus the MAs are determined to be different. As a result, the CC cannot be connected.

To activate the CC, specify configurations separately for IEEE 802.1ag and ITU-T Y.1731.

#### (2) Loopback operation

IEEE 802.1ag and ITU-T Y.1731 differ in whether the TLV is included in loopback messages. The following table describes whether the TLV is in loopback messages.

*Table 11-14: Existence of the TLV in loopback messages*

TLV type	IEEE 802.1ag	ITU-T Y.1731
Sender ID TLV	Y	N

Legend: Y: exists, N: does not exist

Thus, if you execute the loopback functionality compliant with ITU-T Y.1731 on a device compliant with IEEE 802.1ag, it appears that the corresponding TLV is missing in cases in which the remote device collects or displays TLV.

#### (3) Linktrace operation

The information length of the TLV included in a response message for linktrace message differs in IEEE 802.1ag and ITU-T Y.1731. The following table describes the information length of the TLV included in a response message for linktrace message.

*Table 11-15: Information length of the TLV included in a response message for linktrace message*

TLV type	IEEE 802.1ag	ITU-T Y.1731
Reply Ingress TLV	10 or greater.	Fixed value of 7
Reply Egress TLV	10 or greater.	Fixed value of 7

For this reason, the response message might be determined as invalid or might seem to be missing some information depending on devices.

### 11.1.12 Operation in BCU duplex configuration

#### (1) Information to be synchronized in the duplex configuration

The items below are synchronized in the active BCU and standby BCU. The synchronized information is to be applied to the standby BCU so that the information can be used continuously after the switchover of BCUs.

- MEP CCM database
- Linktrace database
- Statistics

#### (2) Operation at the time of switchover

The following table describes the behavior of each type of CFM functionality at the time of switchover.



*Table 11-16: Operation at the time of switchover*

Functionality	Operation at the time of switchover
Continuity check	Continuous monitoring is possible.
Loopback	The command being executed needs to be re-executed.
Linktrace	The command being executed needs to be re-executed.

### 11.1.13 Notes on using CFM

#### (1) *Collecting routing information by using the linktrace functionality*

The linktrace functionality determines the destination port for forwarding linktrace messages by referencing the MEP CCM database. However, correct routing information cannot be collected because the destination port cannot be determined until CC sends or receives a CCM.

#### (2) *Burst reception of CFM PDUs*

The Device might receive CFM PDUs in a burst if the timing for sending CFM PDUs from remote MEPs is accidentally the same. In such a case, if the Device receives 2000 or more CFM PDUs in a short time, the Device might discard CFM PDUs and might detect a failure incorrectly.

If this problem occurs often, adjust the capacity and sending interval for CFM.

## 11.2 Configuration

### 11.2.1 List of configuration commands

The following table describes the configuration commands for CFM.

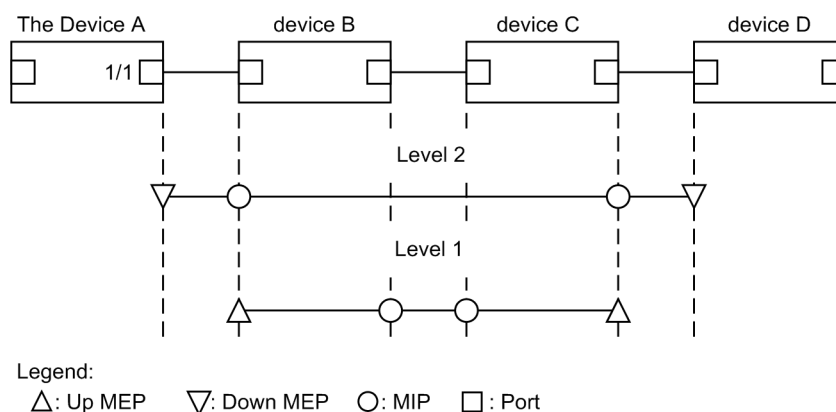
*Table 11-17:* List of configuration commands

Command name	Description
cc alarm-priority	Sets the failure level detected by CC.
cc alarm-reset-time	Sets the period of time until CC recognizes that the failure is a redetected failure.
cc alarm-start-time	Sets the time from the point at which CC detects a failure until it sends a trap.
cc cos	Sets the CoS value for CCM.
cc enable	Sets in a domain an MA in which the CC functionality is used.
cc interval	Sets the CCM sending interval.
domain-name	Sets a domain name.
ethernet cfm ais enable	Stops ETH-AIS by using the <code>no ethernet oam ais enable</code> command.
ethernet cfm cc cos	Sets the CoS value for sending CCM from MEP.
ethernet cfm domain-level	Sets domain and MA for IEEE 802.1ag.
ethernet cfm enable (global)	Starts CFM.
ethernet cfm enable (interface)	Stops CFM by using the <code>no ethernet cfm enable</code> command.
ethernet cfm lck enable	Stops ETH-LCK by using the <code>no ethernet oam lck enable</code> command.
ethernet cfm mel	Sets the MEG for ITU-T Y.1731.
ethernet cfm mep	Sets a MEP used by CFM.
ma-id	Sets the MA ID for IEEE 802.1ag.
meg-id	Sets the MA ID for ITU-T Y.1731.

### 11.2.2 Configuring IEEE 802.1ag CFM

This subsection describes the procedure for configuring a domain for IEEE 802.1ag. Device A is used in the following figure as an example.

Figure 11-30: Configuration example of IEEE 802.1ag CFM



### (1) Setting the domain and an MA

#### Points to note

The level, domain name, and MA ID must match those of the partner device. If these settings are different, the Device and the partner device are not regarded as one MA.

#### Command examples

- ```
(config)# ethernet cfm domain-level 2 ma 2
(config-ether-cfm)# domain-name str operator_2
(config-ether-cfm)# ma-id str BaseA_to_BaseD
(config-ether-cfm)# exit
```

Sets level 2 and MA 2. Also sets the domain name and MA ID.

### (2) Setting a MEP

#### Points to note

Set no more MEPs than the number defined in the capacity limit.

You need to enable the CFM functionality of the device to start using the configured MEP.

#### Command examples

- ```
(config)# interface gigabitethernet 1/1
(config-if)# ethernet cfm mep domain-level 2 ma 2 mep-id 201
(config-if)# exit
```

Sets a MEP belonging to MA 2 of level 2 to port 1/1.

- ```
(config)# ethernet cfm enable
```

Starts operation of CFM on the Device.

### (3) Setting the CC functionality

#### Points to note

The CC functionality starts operation as soon as the `cc enable` command is set.

#### Command examples

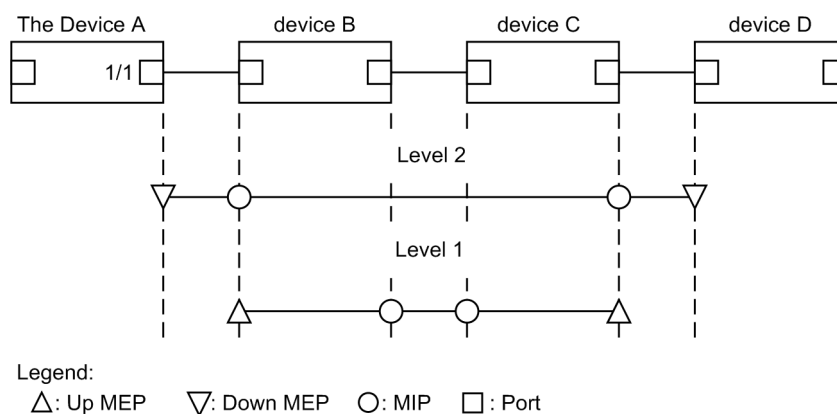
- ```
1. (config)# ethernet cfm domain-level 2 ma 2
   (config-ether-cfm)# cc interval 10sec
   (config-ether-cfm)# cc enable
```

In MA 2 of level 2, sets the CCM sending interval to 10 seconds and starts the CC functionality.

### 11.2.3 Configuring ITU-T Y.1731 CFM

This subsection describes how to configure a domain for ITU-T Y.1731. Device A is used in the following figure as an example.

Figure 11-31: Configuration example of ITU-T Y.1731 CFM



### (1) Setting an MA

### Points to note

The level and MA ID must match those of the partner device. If these settings are different, the Device and the partner device are not regarded as one MA.

## Command examples

1. 

```
(config)# ethernet cfm mel 2 meg 20
```

```
(config-ether-cfm)# meg-id icc 342612 umc TtoO
```

Sets level 2 and MA 20. Also sets the MA ID.

## (2) Setting a MEP

### Points to note

Set no more MEPs than the number defined in the capacity limits.

You need to enable the CFM functionality of the device to start using the configured MEP.

## Command examples

1. 

```
(config)# interface gigabitethernet 1/1
(config-if)# ethernet cfm mep mel 2 meg 20 mep-id 211
(config-if)# exit
```

Sets a MEP belonging to MA 20 of level 2 to port 1/1.
2. 

```
(config)# ethernet cfm enable
```

Starts operation of CFM on the Device.

### (3) Setting the CC functionality

Points to note

The CC functionality starts operation as soon as the `cc enable` command is set.

Command examples

1. 

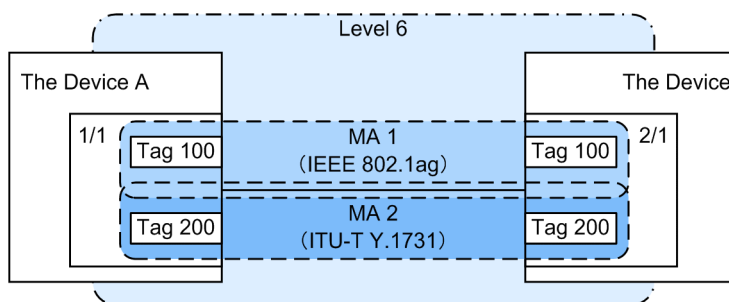
```
(config)# ethernet cfm mel 2 meg 20
(config-ether-cfm)# cc interval 10sec
(config-ether-cfm)# cc enable
```

In MA 20 of level 2, sets the CCM sending interval to 10 seconds and starts the CC functionality.

## 11.2.4 Configuration for using both IEEE 802.1ag and ITU-T Y.1731

This subsection describes the configuration procedure for using both IEEE 802.1ag and ITU-T Y.1731. In Device A in the figure below, MA 1 is configured according to IEEE 802.1ag and MA 2 according to ITU-T Y.1731.

Figure 11-32: CFM configuration example for using both IEEE 802.1ag and ITU-T Y.1731



### (1) Setting MAs for IEEE 802.1ag and ITU-T Y.1731 in the same domain

Points to note

When you set MAs for IEEE 802.1ag and ITU-T Y.1731 in the same domain, make sure that there is no duplication of MA IDs. For important points of basic settings for domains and the MA, see *11.2.2 Configuring IEEE 802.1ag CFM* and *11.2.3 Configuring ITU-T Y.1731 CFM*.

Command examples

1. 

```
(config)# ethernet cfm domain-level 6 ma 1
(config-ether-cfm)# domain-name str customer_6
(config-ether-cfm)# ma-id str Group_1
(config-ether-cfm)# exit
```

Sets the IEEE 802.1ag level and MA. Also sets the domain name and MA ID.

2. 

```
(config)# ethernet cfm mel 6 meg 2
(config-ether-cfm)# meg-id icc 342612 umc Group2
(config-ether-cfm)# exit
```

Sets the ITU-T Y.1731 level and MA. Also sets the MA ID.

**(2) Setting MEPs**

Points to note

MEPs must be set for each MA. For important points of MEP basic settings, see *11.2.2 Configuring IEEE 802.1ag CFM* and *11.2.3 Configuring ITU-T Y.1731 CFM*.

Command examples

1. 

```
(config)# interface gigabitethernet 1/1.100
(config-subif)# ethernet cfm mep domain-level 6 ma 1 mep-id 101
(config-subif)# exit
(config)# interface gigabitethernet 1/1.200
(config-subif)# ethernet cfm mep mel 6 meg 2 mep-id 201
(config-subif)# exit
```

Sets a MEP belonging to MA 1 of level 6 to port 1/1. Also, sets a MEP belonging to MA 2.

2. 

```
(config)# ethernet cfm enable
```

Starts operation of CFM on the Device.

**(3) Setting the CC functionality**

Points to note

The CC functionality starts operation as soon as the `cc enable` command is set.

Command examples

1. 

```
(config)# ethernet cfm domain-level 6 ma 1
(config-ether-cfm)# cc interval 10sec
(config-ether-cfm)# cc enable
(config-ether-cfm)# exit
(config)# ethernet cfm mel 6 meg 2
(config-ether-cfm)# cc interval 10sec
(config-ether-cfm)# cc enable
(config-ether-cfm)# exit
```

Sets the CCM sending interval to 10 seconds and starts the CC functionality.

**11.2.5 Stopping CFM on a port**

Use this configuration to temporarily stop CFM on the ports that are specified for IEEE 802.1ag and ITU-T Y.1731.

Command examples

1. 

```
(config)# interface gigabitethernet 1/1
(config-if)# no ethernet cfm enable
(config-if)# exit
```

Stops CFM on port 1/1.

## 11.3 Operation

### 11.3.1 List of operation commands

The following table describes the operation commands for CFM.

*Table 11-18:* List of operation commands

Command name	Description
l2ping	Executes the CFM loopback functionality and verifies the connectivity between the specified MPs.
l2tracert	Executes the CFM loopback functionality and verifies the routing between the specified MPs.
show cfm	Shows information about a CFM domain.
show cfm remote-mep	Shows information about a CFM remote MEP.
show cfm fault	Shows CFM failure information.
show cfm l2tracert-db	Shows routing information obtained by using the l2tracert command.
show cfm statistics	Shows CFM statistics.
clear cfm remote-mep	Clears remote information about a CFM MEP.
clear cfm fault	Clears CFM failure information.
clear cfm l2tracert-db	Clears routing information obtained by using the l2tracert command.
clear cfm statistics	Clears CFM statistics.
restart cfm	Restarts the CFM program.
dump protocols cfm	Outputs CFM dump information to a file.

### 11.3.2 Checking connection between MPs

Use the `l2ping` command to check the connectivity between the specified MPs and to display the result. For the command, you can specify the number of verifications and the response wait time. By default, the number of verifications is set to 5 times, and the response wait time is set to 5 seconds. When a verification result is returned or the response wait time has elapsed, another verification attempt is started.

*Figure 11-33:* Result of executing the `l2ping` command

```
>l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3 timeout 1
L2ping to MP:1010(0012.e220.00a3) on Level:7 MA:1000 MEP:1020
Time:20XX/03/14 19:10:24 UTC
1: L2ping Reply from 0012.e220.00a3 64bytes Time= 21 ms
2: L2ping Reply from 0012.e220.00a3 64bytes Time= 22 ms
3: L2ping Reply from 0012.e220.00a3 64bytes Time= 23 ms

--- L2ping Statistics ---
Tx L2ping Request : 3 Rx L2ping Reply : 3 Lost Frame : 0%
Round-trip Min/Avg/Max : 21/22/23 ms

>
```

### 11.3.3 Checking the route between MPs

Use the `l2tracert` command to obtain routing information about the route between the specified MPs and to display the result. You can specify the response wait time and a TTL value

for the command. By default, the response wait time is set to 5 seconds, and the TTL value is set to 64.

The word `Hit` confirms that a response from the MP specified as the destination was received.

*Figure 11-34: Result of executing the `l2tracert` command*

```
>l2tracert remote-mep 2010 domain-level 7 ma 1000 mep 2020 timeout 10 ttl 64
Date 20XX/03/15 14:05:30 UTC
L2tracert to MP:0012.e220.00a3 on Level:7 MA:1000 MEP:1020
Time:20XX/03/15 14:05:30 UTC
63 0012.e220.00c0 Forwarded
62 0012.e210.000d Forwarded
61 0012.e242.00a3 NotForwarded Hit
```

### 11.3.4 Checking the state of MPs on a route

You can use the `show cfm l2tracert-db detail` command to check detailed information about the route to the destination MP and the MPs on the route. If the `NotForwarded` message is displayed, you can check the reason that the linktrace message was not forwarded in `Action` on `Ingress Port` and `Egress Port` lines.

*Figure 11-35: Result of executing the `show cfm l2tracert-db detail` command*

```
> show cfm l2tracert-db remote-mac 0012.e220.1040 detail
Date 20XX/03/16 10:21:42 UTC
L2tracert to MP:2010(0012.e220.1040) on Level:7 MA:2000 MEP:2020
Time:20XX/03/16 10:21:42 UTC
63 0012.e220.10a9 Forwarded
  Last Egress : 0012.e210.2400 Next Egress : 0012.e220.10a0
  Relay Action: MacAddrTbl
  Chassis ID   Type: MAC      Info: 0012.e228.10a0
  Ingress Port MP Address: 0012.e220.10a9 Action: OK
  Egress Port  MP Address: 0012.e220.10aa Action: OK
62 0012.e228.aa3b NotForwarded
  Last Egress : 0012.e220.10a0 Next Egress : 0012.e228.aa30
  Relay Action: MacAddrTbl
  Chassis ID   Type: MAC      Info: 0012.e228.aa30
  Ingress Port MP Address: 0012.e228.aa2c Action: -
  Egress Port  MP Address: 0012.e228.aa3b Action: Down
>
```

### 11.3.5 Checking the CFM state

Use the `show cfm operation` command to display the CFM settings and the status of failure detection. If CC has detected a failure in `Status`, you can check the type of the failure that has the highest failure level among the detected failures.

*Figure 11-36: Result of executing the `show cfm` command*

```
>show cfm
Date 20XX/04/01 12:00:00 UTC
Domain Level:3 MA: 100
  Domain Name(str ): ProviderDomain_3
  MA Name(str ): Kanagawa_to_Nagoya
  CC:Enable Interval:1min CoS:7
  Alarm Priority:2 Start Time: 2500ms Reset Time:10000ms
  MEP Information
    ID:6110 DownMEP Port: 1/ 1.1000 (Down) Status:PortState
  MEL:1 MEG: 400
    MEG ID ICC:342612 UMC:TtoO
    CC:Enable Interval:1min CoS:7
    MEP Information
      ID:8110 DownMEP Port:ChGr:768.4000 (Up ) Status:UnexpPeriod
>
```

### 11.3.6 Checking detailed information of failures

Use the `show cfm fault detail` command to display the status of failure detection and the CCM



information. This information is an aid for detecting failures for each failure type. You can check the remote MEP that sent a CCM in RMEP and MAC.

*Figure 11-37: Result of executing the show cfm fault detail command*

```
>show cfm fault detail
Date 20XX/04/01 12:00:00 UTC
MD:7 MA:1000 MEP:1000 Fault
  OtherCCM      :-      RMEP:1001  MAC:0012.e220.11a1  20XX/04/01 11:22:17 UTC
  ErrorCCM      :-
  Timeout       :On  RMEP:1001  MAC:0012.e220.11a1  20XX/04/01 11:42:10 UTC
  PortState     :-
  RDI           :-
MEL:6 MEG: 102 MEP:2010 Fault
  UnexpMEL      :-
  Mismatch      :-
  UnexpMEP      :-
  UnexpPeriod   :On  RMEP: 101  MAC:0012.e220.21a2  20XX/04/01 11:40:04 UTC
  UnexpPriority :-
  LOC           :-
  RDI           :-
  AIS           :-
  LCK           :-
>
```

The remote MEP information displayed by the show cfm fault detail command is an aid in failure detection. In actuality, failures might occur at multiple remote MEPs.

You can use the show cfm remote-mep command to display remote MEP information. Then, you can check the remote MEP where a failure is occurring in ID and Status.

*Figure 11-38: Result of executing the show cfm remote-mep command*

```
>show cfm remote-mep
Date 20XX/04/01 12:00:00 UTC
Total RMEP Counts:      2
Domain Level:3 MA: 100
  Domain Name(str ): ProviderDomain_3
  MA      Name(str ): Kanagawa_to_Nagoya
  MEP ID: 101 (Up ) Port:ChGr: 16      Tag: 100 Status:Timeout
    RMEP Information Counts: 2
    ID:   3  MAC:0012.e220.1224  Status:Timeout      20XX/04/01 07:55:20 UTC
MEL:1 MEG: 400
  MEG ID ICC:342612 UMC:TtoO
  MEP ID: 201 (Up ) Port: 1/21      Tag: 200 Status:-
    RMEP Information Counts: 2
    ID:   5  MAC:0012.e230.1221  Status:-          20XX/04/01 04:21:30 UTC
>
```



## Chapter

---

# 12. LLDP

---

The Link Layer Discovery Protocol (LLDP) functionality detects and manages information about the devices that are neighbors of the Device. This chapter describes LLDP and how to use it.

- 12.1 Description
- 12.2 Configuration
- 12.3 Operation

## 12.1 Description

### 12.1.1 Overview

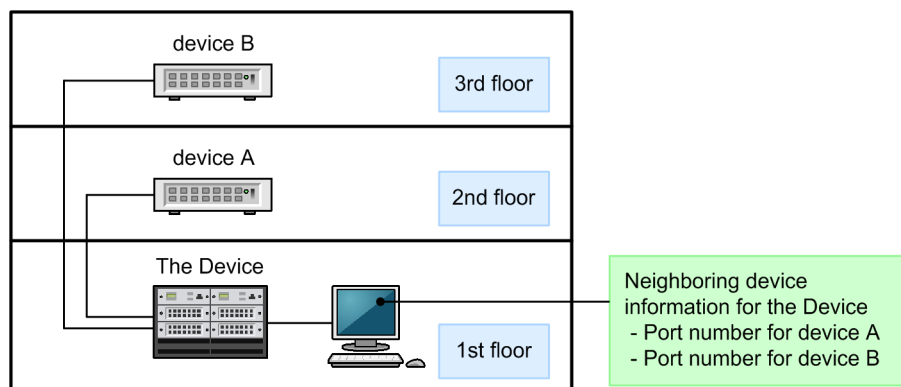
LLDP (Link Layer Discovery Protocol) is a protocol for detecting and managing connections at the data link layer. The information about neighboring devices is automatically detected by sending and receiving LLDP frames (LLDPDU).

#### (1) Example of using LLDP

LLDP is available on all of the Ethernet ports handled by the Device. The ports on which LLDP is enabled manage the information received from the connected devices as neighboring device information.

The figure below shows an example of using LLDP. In this example, the operator of the Device installed on the 1st floor of a building can check the status of connections between the devices installed on other floors of the building.

Figure 12-1: Example of using LLDP



### 12.1.2 Supported specifications

#### (1) Supported LLDP standards

The following two standards are supported on the Device:

- IEEE Std 802.1AB-2009
- IEEE 802.1AB/D6.0 (Draft6.0 LLDP)

By default, the Device operates in IEEE Std 802.1AB-2009 and if a Draft6.0 LLDPDU is received at a port, the port sends out Draft6.0 LLDPDU. Devices compliant with IEEE Std 802.1AB-2005 can also be connected.

#### (2) Supported TLVs

The following table describes the support status for TLV on the Device.

Table 12-1: Support status for TLV

TLV name	Sending	Receiving	Description
Chassis ID	Y	Y	Sends the MAC address of a device.
Port ID	Y	Y	Sends the MAC address of a port.
Time To Live	Y	Y	The retention time for information to be sent by the Device can be changed by using a configuration command.

TLV name	Sending	Receiving	Description
Port Description	Y	Y	Sends the same value as ifDescr of the interface group MIB.
System Name	Y	Y	Sends the same value as sysName of the system group MIB.
System Description	Y	Y	Sends the same value as sysDescr of the system group MIB.
System Capabilities	N	Y	None.
Management Address	N	Y	None.
Organizationally Specific TLVs <ul style="list-style-type: none"> <li>VLAN information</li> <li>VLAN Address information</li> </ul>	Y	Y	Supports Draft6.0 only. Sends and receives the list information of the VLAN tag values and a VLAN tag value corresponding to the IP address.

Legend: Y: Supported, N: Not supported

### 12.1.3 Notes on using LLDP

#### (1) Operation at the time of switchover

When the BCU is switched, information about the neighboring devices are obtained in the new active BCU.

#### (2) Using LLDP with the VRF functionality (Draft6.0)

If the VRF functionality is enabled for a interface, the IP address information set to the interface is not sent.

## 12.2 Configuration

### 12.2.1 List of configuration commands

The following table describes the configuration commands for LLDP.

*Table 12-2:* List of configuration commands

Command name	Description
lldp enable	Enables operation of LLDP for a port.
lldp hold-count	Specifies how long the LLDP frames sent from the Device to neighboring devices will be retained on the neighboring devices.
lldp interval-time	Specifies the interval at which the Device sends LLDP frames.
lldp run	Enables LLDP for the entire device.

### 12.2.2 Configuring LLDP

#### (1) Setting up LLDP

Points to note

LLDP configuration requires enabling LLDP for the entire device, and then enabling LLDP for the port where it will be used.

In the following, LLDP is used for gigabitethernet 1/1.

Command examples

1. **(config)# lldp run**  
Enables LLDP for the entire device.
2. **(config)# interface gigabitethernet 1/1**  
Switches to the configuration command mode for port 1/1.
3. **(config-if)# lldp enable**  
Starts operation of LLDP at port 1/1.

#### (2) Setting the sending interval and retention time of LLDP frames

Points to note

The LLDP frame retention time must be specified as a multiplier of the sending interval.

Command examples

1. **(config)# lldp interval-time 60**  
Sets 60 seconds as the interval for sending LLDP frames.
2. **(config)# lldp hold-count 3**  
Sets the retention time during which the destination-neighboring device will retain the information it received from the Device. The retention time is specified in multiples of the sending interval time. In this example, the retention time is 180 seconds (60 seconds x 3).

## 12.3 Operation

### 12.3.1 List of operation commands

The following table describes the operation commands for LLDP.

*Table 12-3:* List of operation commands

Command name	Description
show lldp	Shows the configuration and neighboring device information for LLDP.
show lldp statistics	Shows LLDP statistics.
clear lldp	Clears LLDP neighboring device information.
clear lldp statistics	Clears LLDP statistics.
restart lldp	Restarts the LLDP program.
dump protocols lldp	Dumps detailed event trace information and control table information collected by the LLDP program to a file.

### 12.3.2 Displaying LLDP information

The `show lldp` command displays the LLDP settings and the number of neighboring devices for each port. The following figure shows the result of executing the command.

*Figure 12-2:* Result of executing the show lldp command

```
> show lldp
Date 20XX/04/01 12:00:00 UTC
Status: Enabled      Chassis ID: Type=MAC      Info=0012.e2c8.3c31
Interval Time: 30    Hold Count: 4      TTL: 121
Port Counts=3
  1/ 1(CH: 10) Link: Up      Neighbor Counts: 1
  1/ 2          Link: Down    Neighbor Counts: 0
  1/ 3          Link: Up      Neighbor Counts: 1
>
```

The detailed information about the neighboring devices is displayed if you execute the `show lldp` command with the `detail` parameter specified. The following figure shows the result of executing the command.

*Figure 12-3:* Result of executing the show lldp command (with the detail parameter specified)

```
> show lldp detail
Date 20XX/04/01 12:00:00 UTC
Status: Enabled      Chassis ID: Type=MAC      Info=0012.e2c8.3c31
Interval Time: 30    Hold Count: 4      TTL: 121      Draft TTL: 120
System Name: LLDP1
System Description: ALAXALA AX8600R AX-8600-R16 [AX8616R] Routing software
(including encryption) Ver. 12.1 [OS-RE]
Neighbor Counts=1
Draft Neighbor Counts=1
Port Counts=3
Port 1/1 (CH: 10)
  Link: Up      PortEnabled: TRUE      AdminStatus: enabledRxTx
  Neighbor Counts: 1      Draft Neighbor Counts: 0
  Port ID: Type=MAC      Info=0012.e238.4cc0
  Port Description: GigabitEthernet 1/1
  Neighbor 1      TTL: 100
    Chassis ID: Type=MAC      Info=0012.e2c8.3c85
    System Name: LLDP2
```

## 12. LLDP

```
System Description: ALAXALA AX8600R AX-8600-R16 [AX8616R] Routing software
(including encryption) Ver. 12.1 [OS-RE]
Port ID: Type=MAC Info=0012.e238.4cd1
Port Description: GigabitEthernet 1/24
Port 1/2
Link: Down PortEnabled: FALSE AdminStatus: enabledRxTx
Neighbor Counts: 0 Draft Neighbor Counts: 0
Port 1/3
Link: Up PortEnabled: TRUE AdminStatus: enabledRxTx
Neighbor Counts: 0 Draft Neighbor Counts: 1
Port ID: Type=MAC Info=0012.e238.4cc2
Port Description: GigabitEthernet 1/3
Tag ID: Tagged=1,10-20,4094
IPv4 Address: Tagged: 10 192.168.248.240
IPv6 Address: Tagged: 20 2001:db8:811:ff01:200:8798:5cc0:e7f4
Draft Neighbor 1 TTL: 100
Chassis ID: Type=MAC Info=0012.e268.2c21
System Name: LLDP3
System Description: ALAXALA AX6300S AX-6300-S08 [AX6308S] Switching software
Ver. 11.9 [OS-SE]
Port ID: Type=MAC Info=0012.e298.5cc4
Port Description: GigabitEthernet 1/5
Tag ID: Tagged=1,10-20,4094
IPv4 Address: Tagged: 10 192.168.248.244
IPv6 Address: Tagged: 20 2001:db8:811:ff01:200:8798:5cc0:e7f8
>
```



---

# Appendix

---

## A. Relevant standards

## A. Relevant standards

### A.1 Policer

*Table A-1:* Relevant standards and recommendations for policer

Name (month and year issued)	Title
RFC 2697 (September 1999)	A Single Rate Three Color Marker
RFC 2698 (September 1999)	A Two Rate Three Color Marker

### A.2 Marker

*Table A-2:* Relevant standard and recommendation for marker

Name (month and year issued)	Title
IEEE 802.1D (June 2004) (IEEE Std 802.1D-2004)	Media Access Control (MAC) Bridges

### A.3 Diff-serv

*Table A-3:* Relevant standards and recommendations for Diff-serv

Name (month and year issued)	Title
RFC 2474 (December 1998)	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475 (December 1998)	An Architecture for Differentiated Services
RFC 2597 (June 1999)	Assured Forwarding PHB Group
RFC 3246 (March 2002)	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC 3260 (April 2002)	New Terminology and Clarifications for Diffserv

### A.4 sFlow

*Table A-4:* Relevant standard and recommendation for sFlow

Name (month and year issued)	Title
RFC 3176 (September 2001)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

### A.5 CFM

*Table A-5:* Relevant standards and recommendations for CFM

Name (month and year issued)	Title
IEEE 802.1ag-2007 (December 2007)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
ITU-T Y.1731 (February 2008)	OAM functions and mechanisms for Ethernet based networks

## A.6 LLDP

*Table A-6:* Relevant standards and recommendations for LLDP

<b>Name (month and year issued)</b>	<b>Title</b>
IEEE 802.1AB/D6.0 (October 2003)	Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery
IEEE Std 802.1AB-2009 (September 2009)	IEEE Standard for Local and metropolitan area networks: Station and Media Access Control Connectivity Discovery



---

# Index

---

## C

CC 128  
CCM 128  
CFM 115  
compliant frames 42  
configuration commands for a QoS flow 37  
configuration commands for CFM 140  
configuration commands for filters 12  
configuration commands for LLDP 152  
configuration commands for port mirroring 92  
configuration commands for port shaper 76  
configuration commands for priority change 66  
configuration commands for QoS control 23  
configuration commands for sFlow statistics 106  
configuration commands for the marker 60  
configuration commands for the policer 46  
continuity check 128

## D

databases used for CFM 136  
detection-condition-oriented mode 3, 29  
domains 120  
Down MEP 121

## E

example of network configuration using filters 2  
example of using LLDP 150

## F

filters 1

## I

implicit discarding 9

## L

linktrace 132  
LLDP 149  
loopback 131

## M

MA 120  
marker 57  
MEP 121  
MIP 122  
mirror port 90  
mirroring 90  
mirroring of received frames 90  
mirroring of sent frames 90  
monitored port 90

monitored session 91

## N

non-compliant frames 42  
notes on using LLDP 151

## O

operation commands common to QoS control 25  
operation commands for a QoS flow 39  
operation commands for CFM 145  
operation commands for filters 18  
operation commands for LLDP 153  
operation commands for port shaper 79  
operation commands for priority change 68  
operation commands for queues in the Device 86  
operation commands for sFlow statistics 113  
operation commands for the marker 62  
operation commands for the policer 52  
overview of functional blocks for QoS control 22  
overview of QoS 21

## P

policer 41  
port mirroring 89  
port shaper 69  
positioning of the marker block 58  
positioning of the policer block 42  
priority change 63

## Q

QoS flow 27  
quantity-oriented mode 3, 29  
queues in the Device 83

## S

sFlow statistics (flow statistics) functionality 95  
structure of QoS control 22  
supported specifications 150

## U

Up MEP 121