AX8600R Software Manual

Configuration Command Reference Vol. 2

For Version 12.1

AX86R-S005X

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-S005X

■ Copyright

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 **- Basic operations (e.g. logging in)** **- Ethernet**	**- Filters and QoS** **- Network management**	**- IP packet forwarding** **- Unicast routing** **- 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
VRRP	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

Preface i

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: Reading the Manual

1. Reading the Manual 1

Command description format 2
Command mode list 3
Specifiable values for parameters 5

PART 2: Filters and QoS

2. Access Lists 11

Number of access lists 12
Names and values that can be specified 15
advance access-group 24
advance access-list 26
advance access-list resequence 27
deny (advance access-list) 29
deny (ip access-list extended) 43
deny (ip access-list standard) 52
deny (ipv6 access-list) 54
deny (mac access-list extended) 62
ip access-group 65
ip access-list extended 67
ip access-list resequence 68
ip access-list standard 70
ipv6 access-list 71
ipv6 access-list resequence 72
ipv6 traffic-filter 74
mac access-group 76
mac access-list extended 78
mac access-list resequence 79
permit (advance access-list) 81
permit (ip access-list extended) 96
permit (ip access-list standard) 105
permit (ipv6 access-list) 107
permit (mac access-list extended) 116
remark 119

3. QoS 121

Number of QoS flow lists and number of policer entries 122

Names and values that can be specified 125
advance qos-flow-group 134
advance qos-flow-list 136
advance qos-flow-list resequence 137
ip qos-flow-group 139
ip qos-flow-list 141
ip qos-flow-list resequence 142
ipv6 qos-flow-group 144
ipv6 qos-flow-list 146
ipv6 qos-flow-list resequence 147
mac qos-flow-group 149
mac qos-flow-list 151
mac qos-flow-list resequence 152
policer 154
qos (advance qos-flow-list) 158
qos (ip qos-flow-list) 174
qos (ipv6 qos-flow-list) 184
qos (mac qos-flow-list) 193
qos-queue-group 197
qos-queue-list 199
remark 202
traffic-shape rate 203

PART 3: Network Management

4. Port Mirroring 205
monitor session 206
5. sFlow Statistics 209
sflow additional-http-port 210
sflow destination 211
sflow extended-information-type 212
sflow forward ingress 214
sflow max-header-size 215
sflow max-packet-size 216
sflow packet-information-type 217
sflow polling-interval 218
sflow sample 219
sflow source 222
6. CFM 223
cc alarm-priority 224
cc alarm-reset-time 226
cc alarm-start-time 227
cc cos 228
cc enable 229
cc interval 230
domain-name 231
ethernet cfm ais enable 233
ethernet cfm cc cos 234
ethernet cfm domain-level 236
ethernet cfm enable (global) 237
ethernet cfm enable (interface) 238
ethernet cfm lck enable 239
ethernet cfm mel 240

ethernet cfm mep 241
ma-id 243
meg-id 244

7. LLDP 247

lldp enable 248
lldp hold-count 249
lldp interval-time 250
lldp run 251

PART 4: Configuration Error Messages

8. Error Messages Displayed When Editing the Configuration 253

8.1 Common errors 254
8.2 Errors when specifying access list settings 255
8.3 Errors when specifying QoS settings 257
8.4 Errors when specifying port mirroring settings 259
8.5 Errors when specifying CFM settings 260
8.6 Errors when specifying LLDP settings 261

Index 263

Chapter

1. Reading the Manual

Command description format
Command mode list
Specifiable values for parameters

Command description format

Each command is described in the following format:

Function

Describes the purpose of the command.

Syntax

Defines the input format of the command. The format is governed by the following rules:

1. Parameters for setting values or character strings are enclosed in angle brackets (`<>`).
2. Characters that are not enclosed in angle brackets (`<>`) are keywords that must be typed exactly as they appear.
3. `{A|B}` indicates that either `A` or `B` must be selected.
4. Parameters or keywords enclosed in square brackets (`[]`) are optional and can be omitted.
5. For details on the parameter input format, see *Specifiable values for parameters*.

Input mode

Indicates the mode required to enter the command. The name of a sub-mode of a configuration command mode corresponds to the name displayed on the command prompt.

Parameters

Describes in detail the parameters that can be set by the command. The default value and the values that can be specified for each parameter are described.

Default behavior

If there are default values for parameters, or a default behavior when a command is not entered, related information is provided here.

Impact on communication

If a setting has an impact on communication, such as interruptions to communication, that impact is described here.

When the change is applied

Describes whether set commands reflected in the running configuration are immediately effective, or whether they take effect only after temporarily stopping operation, such as by restarting the device.

Notes

Provides cautionary information on using the command.

Related commands

Describes the commands that must be set in order to use the applicable command.

Command mode list

The following table lists the command modes.

Table 1-1: Command mode list

No.	Prompt displayed for the command mode	Description	Command for mode transition
1	(config)	Global configuration mode	# configure
2	(config-line)	Configures remote login and console.	(config)# line vty (config)# line console
3	(config-view)	Configures view.	(config)# parser view
4	(config-if)	Configures a management port.	(config)# interface mgmt
		Configures an AUX port.	(config)# interface async
		Configures an Ethernet interface.	(config)# interface gigabitethernet (config)# interface tengigabitethernet (config)# interface hundredgigabitethernet
		Configures a port channel interface.	(config)# interface port-channel
		Configures a loopback interface.	(config)# interface loopback
		Configures a null interface.	(config)# interface null
5	(config-if-range)	Configures multiple Ethernet interfaces.	(config)# interface range gigabitethernet (config)# interface range tengigabitethernet (config)# interface range hundredgigabitethernet
		Configures multiple port channel interfaces.	(config)# interface range port-channel
6	(config-subif)	Configures an Ethernet subinterface.	(config)# interface gigabitethernet (config)# interface tengigabitethernet (config)# interface hundredgigabitethernet (When specified in the subinterface index)
		Configures a port channel subinterface.	(config)# interface port-channel (When specified in the subinterface index)
7	(config-subif-range)	Configures multiple Ethernet subinterfaces.	(config)# interface range gigabitethernet (config)# interface range tengigabitethernet (config)# interface range hundredgigabitethernet (When specified in the subinterface index)
		Configures multiple port channel subinterfaces.	(config)# interface range port-channel (When specified in the subinterface index)
8	(config-adv-acl)	Configures an Advance filter.	(config)# advance access-list
9	(config-ext-nacl)	Configures an IPv4 packet filter.	(config)# ip access-list extended
10	(config-std-nacl)	Configures an IPv4 address filter.	(config)# ip access-list standard
11	(config-ipv6-acl)	Configures an IPv6 filter.	(config)# ipv6 access-list
12	(config-ext-macl)	Configures a MAC filter.	(config)# mac access-list extended

No.	Prompt displayed for the command mode	Description	Command for mode transition
13	(config-adv-qos)	Configures Advance QoS flow.	(config)# advance qos-flow-list
14	(config-ip-qos)	Configures IPv4 QoS flow.	(config)# ip qos-flow-list
15	(config-ipv6-qos)	Configures IPv6 QoS flow.	(config)# ipv6 qos-flow-list
16	(config-mac-qos)	Configures MAC QoS flow.	(config)# mac qos-flow-list
17	(config-msg-list)	Configures message type output conditions.	(config)# message-list <*group name*>
18	(config-ip-pbr)	Configures IPv4 policy-based routing.	(config)# ip policy-list
19	(config-ipv6-pbr)	Configures IPv6 policy-based routing.	(config)# ipv6 policy-list
20	(config-router)	Configures RIP.	(config)# router rip
		Configures OSPF.	(config)# router ospf
		Configures BGP4/BGP4+.	(config)# router bgp
21	(config-router-af)	Configures RIP for each VRF.	(config)# router rip (config-router)# address-family ipv4 vrf
		Configures BGP4 for each VRF. (config-router-af) (ipv4 vrf) mode	(config)# router bgp (config-router)# address-family ipv4 vrf
		Configures BGP4+ global network. (config-router-af) (ipv6) mode	(config)# router bgp (config-router)# address-family ipv6
		Configures BGP4+ for each VRF. (config-router-af) (ipv6 vrf) mode	(config)# router bgp (config-router)# address-family ipv6 vrf
22	(config-route-map)	Configures route-map.	(config)# route-map
23	(config-rtr-rip)	Configures RIPng.	(config)# ipv6 router rip
24	(config-rtr)	Configures OSPFv3.	(config)# ipv6 router ospf
25	(config-vrf)	Configures config-vrf.	(config)# vrf definition
26	(<*Command mode*>-TPL)	Configures the template. template mode <*Command mode*>: Optional command mode	(config)# template
27	(<*Command mode*>-TPL-INS)	Configures the insert position command. insert mode <*Command mode*>: Optional command mode	(<*Command mode*>-TPL)# insert
28	(<*Command mode*>-TPL-REP)	Configures the replace position command. replace mode <*Command mode*>: Optional command mode	(<*Command mode*>-TPL)# replace

Specifiable values for parameters

The following table describes the values that can be specified for parameters.

Table 1-2: Specifiable values for parameters

Parameter type	Description	Input example
Name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for the second and subsequent characters.	neighbor office1 peer-group
Host name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and periods (.) can be used for the second and subsequent characters.	ip host telnet-host 192.168.1.1
Access list name, QoS flow list name, policer entry name, Name of policy-based routing list, QoS queue list name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for the second and subsequent characters.	ip access-list standard inbound1 ip access-list standard 10
Template name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and underscores (_) can be used for the second and subsequent characters.	template tmpl-01-01
Template parameter	Alphanumeric characters, hyphens (-), and underscores (_) can be used.	template tmpl $param-01-01
IPv4 address, Subnet mask	Specify these items in decimal format, separating 1-byte decimal values by a period (.).	192.168.0.14 255.255.255.0
Wildcard mask	The same input format as IPv4 addresses. The set bits in an IPv4 address represent an arbitrary value.	255.255.0.0
IPv6 address	Specify this item in hexadecimal format, separating 2-byte hexadecimal values by colons (:).	2001:db8:1234:5678:9abc:def0:1234:5678 fe80::1
add/remove specification	Add to or delete from the information when multiple interfaces have been specified. The add specification adds information to the current information. The remove specification deletes information from the current information.	monitor session 1 source interface add gigabitethernet 1/1 monitor session 1 source interface remove gigabitethernet 1/1

Any character string

Alphanumeric characters and special characters can be specified for parameters. Some special characters, however, cannot be used. Character codes are listed in the following table. Characters other than alphanumeric characters in the following list of character codes are special characters.

Table 1-3: List of character codes

Character	Code	Character	Code	Character	Code	Character	Code	Character	Code	Character	Code
Space	0x20	0	0x30	@	0x40	P	0x50	`	0x60	p	0x70
!	0x21	1	0x31	A	0x41	Q	0x51	a	0x61	q	0x71
"	0x22	2	0x32	B	0x42	R	0x52	b	0x62	r	0x72
#	0x23	3	0x33	C	0x43	S	0x53	c	0x63	s	0x73
$	0x24	4	0x34	D	0x44	T	0x54	d	0x64	t	0x74
%	0x25	5	0x35	E	0x45	U	0x55	e	0x65	u	0x75
&	0x26	6	0x36	F	0x46	V	0x56	f	0x66	v	0x76
'	0x27	7	0x37	G	0x47	W	0x57	g	0x67	w	0x77
(	0x28	8	0x38	H	0x48	X	0x58	h	0x68	x	0x78
)	0x29	9	0x39	I	0x49	Y	0x59	i	0x69	y	0x79
*	0x2A	:	0x3A	J	0x4A	Z	0x5A	j	0x6A	z	0x7A
+	0x2B	;	0x3B	K	0x4B	[	0x5B	k	0x6B	{	0x7B
,	0x2C	<	0x3C	L	0x4C	\	0x5C	l	0x6C	|	0x7C
-	0x2D	=	0x3D	M	0x4D	]	0x5D	m	0x6D	}	0x7D
.	0x2E	>	0x3E	N	0x4E	^	0x5E	n	0x6E	~	0x7E
/	0x2F	?	0x3F	O	0x4F	_	0x5F	o	0x6F	---	---

Notes

- To enter a question mark (`?`, or 0x3F), press **Ctrl** + **V**, and then type a question mark. You cannot copy and paste any specification string that includes a question mark.

Special characters that cannot be specified

Table 1-4: Special characters that cannot be specified

Character name	Character	Code
Double quotation mark	"	0x22
Dollar sign	$	0x24
Single quotation mark	'	0x27

Character name	Character	Code
Semicolon	;	0x3B
Backslash	\	0x5C
Grave accent mark	`	0x60
Left curly bracket	{	0x7B
Right curly bracket	}	0x7D

Example of specification string

access-list 10 remark "mail:xx@xx %tokyo"

How to specify an interface

The following table describes how to specify the parameters <*interface type*> and <*interface number*> that correspond to the interface type group.

Table 1-5: How to specify an interface

Interface type group	Interface name specified for <*interface type*>	Interface number specified for <*interface number*>
Ethernet interface	gigabitethernet	<*nif no.*>/<*port no.*>
	tengigabitethernet	<*nif no.*>/<*port no.*>
	hundredgigabitethernet	<*nif no.*>/<*port no.*>
Ethernet subinterface	gigabitethernet	<*nif no.*>/<*port no.*>.<*subinterface index*>
	tengigabitethernet	<*nif no.*>/<*port no.*>.<*subinterface index*>
	hundredgigabitethernet	<*nif no.*>/<*port no.*>.<*subinterface index*>
Port channel interface	port-channel	<*channel group number*>
Port channel subinterface	port-channel	<*channel group number*>.<*subinterface index*>
Loopback interface	loopback	0 or <*loopback id*>
Null interface	null	0
Management port	mgmt	0
AUX port	async	1

Specification of multiple interfaces

Use this method to specify the same information for multiple interfaces at the same time. You can specify the interface names and interface numbers that correspond to the following interface type groups from among the groups shown in *Table 1-5: How to specify an interface*.

- Ethernet interface
- Ethernet subinterface
- Port channel interface
- Port channel subinterface

When specifying multiple interfaces, you can specify interfaces that belong to the same interface type group at the same time, but you cannot specify interfaces that belong to different interface groups at the same time.

Syntax

```
interface range <interface type> <interface number>
```

You can specify no more than 16 input formats, separating each by a comma (,).

Input example

```
interface range gigabitethernet 1/1-3
interface range gigabitethernet 1/1-3, tengigabitethernet 3/1
interface range port-channel 2.10-20, port-channel 3.100, port-channel 5.200
```

Range of <sfu no.> values

The following table lists the range of <*sfu no.*> values.

Table 1-6: Range of <sfu no.> values

No.	Model	Range of values
1	All models	1 to 4

Range of <pru no.> values

The following table lists the range of <*pru no.*> values.

Table 1-7: Range of <pru no.> values

No.	Model	Range of values
1	AX8616R	1 to 4
2	AX8632R	1 to 8

Range of <nif no.> and <port no.> values

The following table lists the range of <*nif no.*> values.

Table 1-8: Range of <nif no.> values

No.	Model	Range of values
1	AX8616R	1 to 16
2	AX8632R	1 to 32

The following tables list the range of <*port no.*> values for each NIF.

Table 1-9: Range of <port no.> values

No.	NIF name	Range of values
1	NL1G-12T	1 to 12
2	NL1G-12S	1 to 12
3	NLXG-6RS	1 to 6
4	NMCG-1C	1

Range of values that can be set for <channel group number>

The following table lists the range of <*channel group number*> values.

Table 1-10: Range of <channel group number> values

No.	Model	Range of values
1	AX8616R	1 to 192

No.	Model	Range of values
2	AX8632R	1 to 384

Range of <subinterface index> values

The range of <*subinterface index*> values is from 1 to 65535.

Range of values that can be set for <vlan id>

The following table lists the range of <*vlan id*> values.

Table 1-11: Range of <vlan id> values

No.	Range of values
1	1 to 4095

How to specify <interface id list> and the range of specifiable values

In <*interface id list*>, you can specify several interfaces of the following Ethernet types by using hyphens (-) and commas (,). You can also specify a single interface by omitting what is inside the brackets [ ]. The range of permitted values is the same as the range of <*nif no.*> and <*port no.*> values in the above tables.

- For gigabit Ethernet interfaces

  gigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>]

- For 10 gigabit Ethernet interfaces

  tengigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>]

- For 100 gigabit Ethernet interfaces

  hundredgigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>]

Example of a range specification that uses a hyphen (-) and comma (,):

gigabitethernet 1/1-2,gigabitethernet 1/5,tengigabitethernet 3/1

Range of values that can be set for <vrf id>

The following table lists the range of <*vrf id*> values.

Table 1-12: Range of <vrf id> values

No.	Range of values
1	1 to 1024

Specifiable values for <message type>

The following table lists the values that can be specified for <*message type*>.

Table 1-13: Range of <message type> values

No.	Specifiable values
1	BCU
2	SFU
3	PRU
4	NIF
5	PS

No.	Specifiable values
6	FAN
7	KEY
8	CONFIGERR
9	CMDRSP
10	SOFTWARE
11	CONFIG
12	ACCESS
13	NTP
14	SOP-KEY
15	SOP-RSP
16	SNMP
17	PORT
18	ChGr
19	CFM
20	IP
21	PBR
22	DHCP
23	VRRP
24	RIP
25	RIPng
26	OSPF
27	OSPFv3
28	BGP4
29	BGP4+
30	UNICAST
31	PIM-IPv4
32	IGMP
33	PIM-IPv6
34	MLD
35	MULTI-IPv4
36	MULTI-IPv6
37	MULTI-INFO

Chapter
2. Access Lists

Number of access lists
Names and values that can be specified
advance access-group
advance access-list
advance access-list resequence
deny (advance access-list)
deny (ip access-list extended)
deny (ip access-list standard)
deny (ipv6 access-list)
deny (mac access-list extended)
ip access-group
ip access-list extended
ip access-list resequence
ip access-list standard
ipv6 access-list
ipv6 access-list resequence
ipv6 traffic-filter
mac access-group
mac access-list extended
mac access-list resequence
permit (advance access-list)
permit (ip access-list extended)
permit (ip access-list standard)
permit (ipv6 access-list)
permit (mac access-list extended)
remark

Number of access lists

Number of access lists

The number of access lists is the number of names that can be used as access list IDs. A maximum of 100608 lists can be created for <*access list name*> of a relevant configuration.

Number of sequences

The number of sequences is the total of the implicit discarded entries with the `permit` command and `deny` command.

A maximum of 256000 entries can be created for all access lists. The number of sequences here also includes the number of sequences of the QoS flow list.

Number of access lists that can be set for an interface

The number of access lists that can be set for an interface is the total number of access lists that can be set for the interface. A maximum of 100608 lists can be created.

If an access list is created and is not set for the interface, this access list is not counted in the number of access lists that can be set for the interface.

If a single access list is set for multiple interfaces, each list is counted as a separate list.

If multiple access lists are set for a single interface, each list is counted as a separate list. In this case, the receiving side and sending side are each counted as separate lists. For example, if an access list is set for both the receiving side and sending side of the same interface, two lists are counted regardless of whether the same access list name is specified.

Number of sequences that can be set for an interface

The number of sequences that can be set for an interface refers to the total number of sequences that can be set for an interface. A maximum of 256000 entries can be created. The number of sequences here also includes the number of sequences that can be set for the interfaces of QoS flow lists.

If an access list where a sequence has not been set is set for an interface, this access list is not counted in the number of sequences that can be set for the interface.

If an access list where a sequence has been set is set for an interface, it is counted as a separate entry for each access list that is set for the interface even if the access list name is the same.

Examples of calculating the number of access lists and number of sequences

The following table describes examples of calculating the number of access lists and the number of sequences.

Table 2-1: Examples of calculating the number of access lists and number of sequences

Sample code	Number of access lists to be used	Number of access lists that can be set for an interface to be used	Number of sequences to be used	Number of sequences that can be set for an interface to be used

In this example, access list `AAA` is created and applied to inbound on Ethernet interface 1/1.
`interface gigabitethernet 1/1`
` ip access-group AAA in`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
	1 list	1 list	3 entries	3 entries

In this example, access list `AAA` is created and applied to inbound on Ethernet interfaces 1/1 and 1/2.
`interface gigabitethernet 1/1`
` ip access-group AAA in`
 	
`interface gigabitethernet 1/2`
` ip access-group AAA in`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
	1 list	2 lists	3 entries	6 entries

In this example, access list `AAA` is created and applied to inbound and outbound on Ethernet interface 1/1.
`interface gigabitethernet 1/1`
` ip access-group AAA in`
` ip access-group AAA out`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
	1 list	2 lists	3 entries	6 entries

In this example, access list `AAA` is created and applied to inbound on Ethernet interface 1/1.
In this example, access list `BBB` is created and applied to inbound on Ethernet interface 1/2.
`interface gigabitethernet 1/1`
` ip access-group AAA in`
 	
`interface gigabitethernet 1/2`
` ip access-group BBB in`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
 	
`ip access-list extended BBB`
` 10 permit udp any any`
` 20 deny tcp any any`
	2 lists	2 lists	6 entries	6 entries

Sample code	Number of access lists to be used	Number of access lists that can be set for an interface to be used	Number of sequences to be used	Number of sequences that can be set for an interface to be used

In this example, access list AAA is created and applied to inbound on Ethernet interface 1/1.
In this example, access list BBB is created and applied to outbound on Ethernet interface 1/1.
`interface gigabitethernet 1/1`
` ip access-group AAA in`
` ip access-group BBB out`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
 	
`ip access-list extended BBB`
` 10 permit udp any any`
` 20 deny tcp any any`
	2 lists	2 lists	6 entries	6 entries

In this example, access list AAA is created but not applied to any interface.
`ip access-list extended AAA`
` 10 permit tcp any any`
	1 list	0 list	2 entries	0 entry

Names and values that can be specified

Protocol names (IPv4)

The following table lists the names that can be specified as IPv4 protocol names.

Table 2-2: Protocol names that can be specified (IPv4)

Protocol name	Applicable protocol number
ah	51
esp	50
gre	47
icmp	1
igmp	2
ip	All IP protocols
ipinip	4
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	41
udp	17
vrrp	112

Protocol names (IPv6)

The following table lists the names that can be specified as IPv6 protocol names.

Table 2-3: Protocol names that can be specified (IPv6)

Protocol name	Applicable protocol number
gre	47
icmp	58
ipv6	All IP protocols
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	4
udp	17

Protocol name	Applicable protocol number
vrrp	112

Port names (TCP)

The following table lists the port names that can be specified for TCP.

Table 2-4: Port names that can be specified for TCP

Port name	Applicable port name and number
bgp	Border Gateway Protocol version 4 (179)
chargen	Character generator (19)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
exec	Remote process execution (512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (20)
gopher	Gopher (70)
hostname	NIC Host Name Server (101)
http	HyperText Transfer Protocol (80)
https	HTTP over TLS/SSL (443)
ident	Ident Protocol (113)
imap3	Interactive Mail Access Protocol version 3 (220)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)
lpd	Printer service (515)
nntp	Network News Transfer Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
pop3s	POP3 over TLS/SSL (995)
raw	Printer PDL Data Stream (9100)
shell	Remote commands (514)
smtp	Simple Mail Transfer Protocol (25)

Port name	Applicable port name and number
smtps	SMTP over TLS/SSL (465)
ssh	Secure Shell Remote Login Protocol (22)
sunrpc	Sun Remote Procedure Call (111)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nicname (43)

Port names (UDP)

The following table lists the port names that can be specified for UDP.

Table 2-5: Port names that can be specified for UDP (IPv4)

Port name	Applicable port name and number
biff	Biff (512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)

Port name	Applicable port name and number
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

Table 2-6: Port names that can be specified for UDP (IPv6)

Port name	Applicable port name and number
biff	Biff (512)
dhcpv6-client	DHCPv6 client (546)
dhcpv6-server	DHCPv6 server (547)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
ripng	Routing Information Protocol next generation (521)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

tos names

The following table lists the tos names that can be specified.

Table 2-7: tos names that can be specified

tos name	tos value
max-reliability	2
max-throughput	4
min-delay	8
min-monetary-cost	1
normal	0

precedence names

The following table lists the precedence names that can be specified.

Table 2-8: precedence names that can be specified

precedence name	precedence value
critical	5
flash	3
flash-override	4
immediate	2
internet	6
network	7
priority	1
routine	0

DSCP names

The following table lists the DSCP names that can be specified.

Table 2-9: DSCP names that can be specified

DSCP name	DSCP value
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38

DSCP name	DSCP value
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
default	0
ef	46

Ethernet type names

The following table lists the Ethernet type names that can be specified.

Table 2-10: Ethernet type names that can be specified

Ethernet type name	Ethernet value	Remarks
appletalk	0x809b	
arp	0x0806	
axp	0x88f3	Alaxala Protocol
eapol	0x888e	
gsrp	--#	Displays GSRP control packets.
ipv4	0x0800	
ipv6	0x86dd	
ipx	0x8137	
xns	0x0600	

#: The value is not made public.

Destination MAC address names

The following table lists the destination MAC address names that can be specified.

Table 2-11: Destination MAC address names that can be specified

Destination address specification	Destination address	Destination address mask
bpdu	0180.C200.0000	0000.0000.0000
broadcast	FFFF.FFFF.FFFF	0000.0000.0000
cdp	0100.0CCC.CCCC	0000.0000.0000
lldp	0180.C200.000E	0000.0000.0000
multicast#	0100.0000.0000	FEFF.FFFF.FFFF
oadp	0100.4C79.FD1B	0000.0000.0000

Destination address specification	Destination address	Destination address mask
pvst-plus-bpdu	0100.0CCC.CCCD	0000.0000.0000
slow-protocol	0180.C200.0002	0000.0000.0000

#: Includes broadcast packets.

Message names (ICMP)

The following table lists the message names that can be specified for ICMP.

Table 2-12: Message names that can be specified for ICMP (IPv4)

Message name	Message	Type	Code
administratively-prohibited	Administratively prohibited	3	13
alternate-address	Alternate address	6	Not specified
conversion-error	Datagram conversion	31	Not specified
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	Not specified
echo-reply	Echo reply	0	Not specified
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1
information-reply	Information replies	16	Not specified
information-request	Information requests	15	Not specified
mask-reply	Mask replies	18	Not specified
mask-request	Mask requests	17	Not specified
mobile-redirect	Mobile host redirect	32	Not specified
net-redirect	Network redirect	5	0
net-tos-redirect	Network redirect for TOS	5	2
net-tos-unreachable	Network unreachable for TOS	3	11
net-unreachable	Network unreachable	3	0
network-unknown	Network unknown	3	6
no-room-for-option	Parameter required but no room	12	2

Message name	Message	Type	Code
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4
parameter-problem	All parameter problems	12	Not specified
port-unreachable	Port unreachable	3	3
precedence-unreachable	Precedence cutoff	3	15
protocol-unreachable	Protocol unreachable	3	2
reassembly-timeout	Reassembly timeout	11	1
redirect	All redirects	5	Not specified
router-advertisement	Router discovery advertisements	9	Not specified
router-solicitation	Router discovery solicitations	10	Not specified
source-quench	Source quenches	4	Not specified
source-route-failed	Source route failed	3	5
time-exceeded	All time exceeded	11	Not specified
timestamp-reply	Timestamp replies	14	Not specified
timestamp-request	Timestamp requests	13	Not specified
traceroute	Traceroute	30	Not specified
ttl-exceeded	TTL exceeded	11	0
unreachable	All unreachable	3	Not specified

Table 2-13: Message names that can be specified for ICMP (IPv6)

Message name	Message	Type	Code
beyond-scope	Destination beyond scope	1	2
destination-unreachable	Destination address is unreachable	1	3
echo-reply	Echo reply	129	Not specified
echo-request	Echo request (ping)	128	Not specified
header	Parameter header problems	4	0
hop-limit	Hop limit exceeded in transit	3	0
mld-query	Multicast Listener Discovery Query	130	Not specified
mld-reduction	Multicast Listener Discovery Reduction	132	Not specified
mld-report	Multicast Listener Discovery Report	131	Not specified
nd-na	Neighbor discovery neighbor advertisements	136	Not specified
nd-ns	Neighbor discovery neighbor solicitations	135	Not specified
next-header	Parameter next header problems	4	1
no-admin	Administration prohibited destination	1	1

Message name	Message	Type	Code
no-route	No route to destination	1	0
packet-too-big	Packet too big	2	Not specified
parameter-option	Parameter option problems	4	2
parameter-problem	All parameter problems	4	Not specified
port-unreachable	Port unreachable	1	4
reassembly-timeout	Reassembly timeout	3	1
renum-command	Router renumbering command	138	0
renum-result	Router renumbering result	138	1
renum-seq-number	Router renumbering sequence number reset	138	255
router-advertisement	Neighbor discovery router advertisements	134	Not specified
router-renumbering	All router renumbering	138	Not specified
router-solicitation	Neighbor discovery router solicitations	133	Not specified
time-exceeded	All time exceeded	3	Not specified
unreachable	All unreachable	1	Not specified

advance access-group

Applies an Advance access list to an interface, and enables the Advance filtering functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

If you apply an access list with the policy-based routing parameter specified, specify the inbound (receiving) side.

Syntax

To set information:

```
advance access-group <access list name> {in | out}
```

To delete information:

```
no advance access-group <access list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<access list name>

Specifies the access list name of the Advance filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

When an access list with at least one entry is removed from an interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This can be set if the flow detection mode is condition-oriented.
2. One can be set for each inbound and outbound side of the same interface. If it is already set, delete before specifying the setting.
3. If a non-existent Advance filter is set, no action is performed. The access list name of the Advance filter is registered.
4. This can be set if an IPv4 address is set for the target interface when `mac-ip` is specified for the flow detection condition type, and there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
5. This can be set if a single IPv6 global address only is set for the target interface when `mac-ipv6` is specified for the flow detection condition type, and there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
6. If policy-based routing is specified, the IPv4 address that is set for the target interface cannot be set for the destination IPv4 address of the flow detection conditions.
7. If policy-based routing is specified, the IPv6 global address that is set for the target interface cannot be set for the destination IPv6 address of the flow detection conditions.

Related commands

```
advance access-list
flow detection mode
```

advance access-list

Sets an access list to be used as an Advance filter. After this command is executed, the mode changes to `config-adv-acl` mode.

Syntax

To set information:

```
advance access-list <access list name>
```

To delete information:

```
no advance access-list <access list name>
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the access list name of the Advance filter.

Access list names that are already being used in the IPv4 address filter, IPv4 packet filter, IPv6 filter, and MAC filter cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

When an access list with at least one entry that was already applied to an interface is removed from the interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
advance access-group
advance access-list resequence
deny (advance access-list)
permit (advance access-list)
remark
```

advance access-list resequence

Re-sequences the sequence numbers that determine the order in which the Advance filter applies flow detection conditions.

Syntax

To set or change information:

```
advance access-list resequence <access list name> [<starting sequence>
[<increment sequence>]]
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies an access list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
advance access-list
```

deny (advance access-list)

Specifies the conditions by which the Advance filter denies access.

Syntax

To set or change information:

```
[<sequence>] deny mac <target flow>
[<sequence>] deny mac-ip <target flow>
[<sequence>] deny mac-ipv6 <target flow>
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

For `mac` *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions.

```
mac {<source mac> <source mac mask> | host <source mac> | any} {<destination
mac> <destination mac mask> | host <destination mac> | any | <destination mac
name>} [<ethernet type>] [{untagged | [user-priority <priority>] [tag-vlan
<vlan id>]}]
```

For `mac-ip` *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions, VLAN Tag header conditions, IPv4 header conditions, or Layer 4 header conditions.

If the `+fo` parameter is set for the flow detection conditions, the MAC header conditions, VLAN tag header conditions, and IPv4 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, ICMP, and IGMP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ip | <protocol>} {{<source ipv4> |
own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address}
| any | own-prefix | range-address <source ipv4 start> <source ipv4 end>}
{{<destination ipv4> | own-address} <destination ipv4 wildcard> | host
{<destination ipv4> | own-address} | any | own-prefix | range-address
<destination ipv4 start> <destination ipv4 end>} [{[tos <tos>]
[precedence <precedence>] | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} tcp {{<source ipv4> | own-address} <source ipv4
wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source
port> | range <source port start> <source port end>}] {{<destination
ipv4> | own-address} <destination ipv4 wildcard> | host {<destination
ipv4> | own-address} | any | own-prefix | range-address <destination ipv4
start> <destination ipv4 end>} [{{eq | neq} <destination port> | range
<destination port start> <destination port end>}] [{[established] |
[{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}] [{+rst | -rst}] [{+syn |
-syn}] [{+urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp
<dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged
| [user-priority <priority>] [tag-vlan <vlan id>]}]
```

When the `+fo` parameter is not specified and the upper layer protocol is UDP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} udp {{<source ipv4> | own-address} <source ipv4
wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source
port> | range <source port start> <source port end>}] {{<destination
ipv4> | own-address} <destination ipv4 wildcard> | host {<destination
ipv4> | own-address} | any | own-prefix | range-address <destination ipv4
start> <destination ipv4 end>} [{{eq | neq} <destination port> | range
<destination port start> <destination port end>}] [{[tos <tos>]
[precedence <precedence>] | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the `+fo` parameter is not specified and the upper layer protocol is ICMP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} icmp {{<source ipv4> | own-address} <source
ipv4 wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4>
| own-address} <destination ipv4 wildcard> | host {<destination ipv4> |
own-address} | any | own-prefix | range-address <destination ipv4 start>
<destination ipv4 end>} [{<icmp type> [<icmp code>] | <icmp message>}]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority
<priority>] [tag-vlan <vlan id>]}]
```

When the `+fo` parameter is not specified and the upper layer protocol is IGMP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} igmp {{<source ipv4> | own-address} <source
ipv4 wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4>
| own-address} <destination ipv4 wildcard> | host {<destination ipv4> |
own-address} | any | own-prefix | range-address <destination ipv4 start>
<destination ipv4 end>} [<igmp type>] [{[tos <tos>] [precedence
<precedence>] | dscp <dscp>}] [length {upper | lower} <length>] [{+mf |
-mf}] [-fo] [{untagged | [user-priority <priority>] [tag-vlan <vlan
id>]}]
```

When the `+fo` parameter is specified:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ip | <protocol> | icmp | igmp | tcp | udp}
{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4
start> <source ipv4 end>} {{<destination ipv4> | own-address}
<destination ipv4 wildcard> | host {<destination ipv4> | own-address} |
any | own-prefix | range-address <destination ipv4 start> <destination
ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
[user-priority <priority>] [tag-vlan <vlan id>]}]
```

For `mac-ipv6` *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions, VLAN Tag header conditions, IPv6 header conditions, or Layer 4 header conditions.

If the `+fo` parameter is set for the flow detection conditions, the MAC header conditions, VLAN tag header conditions, and IPv6 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

When the +fo parameter is not specified and the upper layer protocol is a type other than TCP, UDP, and ICMP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ipv6 | <protocol>} {<source ipv6>/<length>|
host {<source ipv6> | own-address} | any | own-address <own address
length> | own-prefix | range-address <source ipv6 start> <source ipv6
end>} {<destination ipv6>/<length>| host {<destination ipv6> |
own-address} | any | own-address <own address length> | own-prefix |
range-address <destination ipv6 start> <destination ipv6 end>}
[{traffic-class <traffic class> | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is TCP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} tcp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any| own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq}
<source port> | range <source port start> <source port end>}]
{<destination ipv6>/<length>| host {<destination ipv6> | own-address} |
any | own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port
end>}] [{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}]
[{+rst | -rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{traffic-class
<traffic class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf
| -mf}] [-fo] [{untagged | [user-priority <priority>] [tag-vlan <vlan
id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is UDP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} udp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any | own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq}
<source port> | range <source port start> <source port end>}]
{<destination ipv6>/<length>| host {<destination ipv6> | own-address} |
any | own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port
end>}] [{traffic-class <traffic class> | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority
<priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is ICMP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} icmp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any | own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} {<destination
ipv6>/<length>| host {<destination ipv6> | own-address} | any |
own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp
code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged |
[user-priority <priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is specified:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ipv6 | <protocol> | icmp | tcp | udp} {<source
ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address
<own address length> | own-prefix | range-address <source ipv6 start>
<source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6>
| own-address} | any | own-address <own address length> | own-prefix |
range-address <destination ipv6 start> <destination ipv6 end>}
[{traffic-class <traffic class> | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [+fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

Input mode

`(config-adv-acl)`

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{*<source mac>* *<source mac mask>* | host *<source mac>* | any}

Specifies the source MAC address.

If `host` *<source mac>* is specified, the flow detection condition is an exact match of *<source mac>*.

To specify all source MAC addresses, specify `any`. If `any` is specified, the source MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source MAC address for *<source mac>*.

   For *<source mac mask>*, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{*<destination mac>* *<destination mac mask>* | host *<destination mac>* | any | *<destination mac name>}*

Specifies the destination MAC address.

If `host` *<destination mac>* is specified, the flow detection condition is an exact match of *<destination mac>*.

To specify all destination MAC addresses, specify `any`. If `any` is specified, the destination MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Specify the destination MAC address for <*destination mac*>.

For <*destination mac mask*>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

Specify the destination MAC address for <*destination mac name*>. For details about the destination MAC address names that can be specified, see *Table 2-11: Destination MAC address names that can be specified*.

MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<*ethernet type*>

Specifies the Ethernet type number.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name.

   For details about the Ethernet type names that can be specified, see *Table 2-10: Ethernet type names that can be specified*.

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

tag-vlan <*vlan id*>

Specifies the VLAN ID of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 4095 in decimal.

{ip | <*protocol*> | icmp | igmp | tcp | udp}

You can select this parameter when `mac-ip` is specified as the flow detection condition.

Specifies the upper-layer protocol condition for IPv4 packets. Note that if all protocols are applicable, specify `ip`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set 0 to 255 (in decimal) or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-2: Protocol names that can be specified (IPv4)*.

{ipv6 | <*protocol*> | icmp | tcp | udp}

You can select this parameter when `mac-ipv6` is specified as the flow detection condition.

Specifies the upper-layer protocol condition for IPv6 packets. Note that if all protocols are applicable, specify `ipv6`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 42, 45 to 49, 52 to 59, 61 to 255 (in decimal), or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-3: Protocol names that can be specified (IPv6)*.

{{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>}

Specifies the source IPv4 address.

If `host` <*source ipv4*> is specified, the flow detection condition is an exact match of <*source ipv4*>.

To specify all source IPv4 addresses, specify `any`. If `any` is specified, the source IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the source IPv4 address.

If own-prefix is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*source ipv4 start*> to <*source ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv4 address for <*source ipv4*>.

   For <*source ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*source ipv4 end*> is larger than <*source ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*source ipv6 start*> <*source ipv6 end*>}

Specifies the source IPv6 address.

If `host` <*source ipv6*> is specified, the flow detection condition is an exact match of <*source ipv6*>.

To specify all source IPv6 addresses, specify `any`. If `any` is specified, the source IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the source IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the source IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*source ipv6 start*> to <*source ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv6 address for <*source ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

   Specify IPv6 addresses so that <*source ipv6 end*> is larger than <*source ipv6 start*>.

   <*source ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <*length*>: 0 to 128

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be specified, see *Table 2-4: Port names that can be specified for TCP*, *Table 2-5: Port names that can be specified for UDP (IPv4)*, or *Table 2-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

If `host` *<destination ipv4>* is specified, the flow detection condition is an exact match of *<destination ipv4>*.

To specify all destination IPv4 addresses, specify `any`. If `any` is specified, the destination IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the target IPv4 address.

If `own-prefix` is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from *<destination ipv4 start>* to *<destination ipv4 end>*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv4 address for *<destination ipv4>*.

   For *<destination ipv4 wildcard>*, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that *<destination ipv4 end>* is larger than *<destination ipv4 start>*.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{*<destination ipv6>/<length>*| host {*<destination ipv6>* | own-address} | any | own-address *<own address length>* | own-prefix | range-address *<destination ipv6 start> <destination ipv6 end>*}

Specifies the destination IPv6 address.

If `host` *<destination ipv6>* is specified, the flow detection condition is an exact match of *<destination ipv6>*.

To specify all destination IPv6 addresses, specify `any`. If `any` is specified, the destination IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the target IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the target IPv6 address and IPv6 global address for *<length>*.

If `range-address` is specified, the flow detection condition is in the range from *<destination ipv6 start>* to *<destination ipv6 end>*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv6 address for *<destination ipv6>*.

   For *<length>*, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For *<own address length>*, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

Specify IPv6 addresses so that <*destination ipv6 end*> is larger than <*destination ipv6 start*>.

<*destination ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<*length*>: 0 to 128

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*destination port*>.

If `neq` is specified, the flow detection condition is other than <*destination port*>.

If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be specified, see *Table 2-4: Port names that can be specified for TCP*, *Table 2-5: Port names that can be specified for UDP (IPv4)*, or *Table 2-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

tos <*tos*>

Specifies 4 bits (bits 3 to 6) in the ToS field as the tos value.

The TOS value is compared with 4 bits (bits 3 to 6) in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 2-7: tos names that can be specified*.

precedence <*precedence*>

Specifies the precedence value, which is the first 3 bits in the ToS field.

Its value is compared with the first 3 bits in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 2-8: precedence names that can be specified*.

traffic-class <*traffic class*>

Specifies the traffic class field value.

Its value is compared with the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

dscp <*dscp*>

- When the flow detection condition type is `mac-ip`:

  Specifies the DSCP value, which is the first 6 bits in the ToS field.

  Its value is compared with the first 6 bits in the ToS field of the received packet.

- When the flow detection condition type is `mac-ipv6`:

  Specifies the DSCP value, which is the first 6 bits in the traffic class field.

  Its value is compared with the first 6 bits in the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 2-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<icmp type>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp code>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp message>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be set, see *Table 2-12: Message names that can be specified for ICMP (IPv4)* or *Table 2-13: Message names that can be specified for ICMP (IPv6)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<igmp type>

Specifies the IGMP type.

This parameter option is available only if the protocol is IGMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

length {upper | lower} *<length>*

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of *<length>* or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of <*length*> or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

- When the flow detection condition type is `mac-ip`:

  Specifies the MF flag value, which is the lower 1 bit in the Flags field.

  `+mf` indicates a packet where an MF flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an MF flag of 0 is set for the flow detection conditions.

- When the flow detection condition type is `mac-ipv6`:

  Specifies the M flag value of the fragment header.

  `+mf` indicates a packet where an M flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an M flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If *nnnn*.*nnnn*.*nnnn* `ffff.ffff.ffff` is entered as the source MAC address and the destination MAC address, `any` is displayed.

2. If the destination MAC address name or the address of the destination MAC address name is entered for the destination MAC address, the destination MAC address name is displayed.

   If *nnnn*.*nnnn*.*nnnn* `0000.0000.0000` is entered as the source MAC address and the destination MAC address in cases other than the above, `host` *nnnn.nnnn.nnnn* is displayed.

3. If `255.255.255.255` is entered for the source IPv4 address wildcard mask and the destination IPv4 address wildcard mask, `any` is displayed.
4. If `0.0.0.0` is entered for the source IPv4 address wildcard mask and the destination IPv4 address wildcard mask, `host` *nnn*.*nnn*.*nnn*.*nnn*, `host own-address` is displayed.
5. If 0 is entered for the <*length*> or <*own address length*> of the source IPv6 address and destination IPv6 address, `any` is displayed.
6. If 128 is entered for the <*length*> or <*own address length*> of the source IPv6 address and destination IPv6 address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*, `host own-address` is displayed.

Related commands

```
advance access-group
advance access-list resequence
permit (advance access-list)
remark
```

deny (ip access-list extended)

Specifies the conditions by which the IPv4 packet filter denies access.

If the `+fo` parameter is set for the flow detection conditions, the VLAN tag header conditions and IPv4 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

Syntax

To set or change information:

```
[<sequence>] deny <target flow>
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, ICMP, and IGMP:

```
{ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> |
host {<source ipv4> | own-address} | any | own-prefix | range-address <source
ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address}
<destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any
| own-prefix | range-address <destination ipv4 start> <destination ipv4 end>}
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} [{{eq | neq} <source port> | range <source port start>
<source port end>}] {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port end>}]
[{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}] [{+rst |
-rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{[tos <tos>] [precedence
<precedence>] | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}]
[-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is UDP:

```
udp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} [{{eq | neq} <source port> | range <source port start>
<source port end>}] {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port end>}]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is ICMP:

```
icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{<icmp type>
[<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] |
dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged
| user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is IGMP:

```
igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is specified:

```
{ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address}
<source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own-prefix
| range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4>
| own-address} <destination ipv4 wildcard> | host {<destination ipv4> |
own-address} | any | own-prefix | range-address <destination ipv4 start>
<destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp
<dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
user-priority <priority>}]
```

Input mode

```
(config-ext-nacl)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{ip | *<protocol>* | icmp | igmp | tcp | udp}

Specifies the upper-layer protocol condition for IPv4 packets. Note that if all protocols are applicable, specify `ip`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set 0 to 255 (in decimal) or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-2: Protocol names that can be specified (IPv4)*.

{{*<source ipv4>* | own-address} *<source ipv4 wildcard>* | host {*<source ipv4>* | own-address} | any | own-prefix | range-address *<source ipv4 start>* *<source ipv4 end>*}

Specifies the source IPv4 address.

If `host` *<source ipv4>* is specified, the flow detection condition is an exact match of *<source ipv4>*.

To specify all source IPv4 addresses, specify `any`. If `any` is specified, the source IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the source IPv4 address.

If own-prefix is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*source ipv4 start*> to <*source ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv4 address for <*source ipv4*>.

   For <*source ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*source ipv4 end*> is larger than <*source ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-5: Port names that can be specified for UDP (IPv4)*.

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

If `host` <*destination ipv4*> is specified, the flow detection condition is an exact match of <*destination ipv4*>.

To specify all destination IPv4 addresses, specify `any`. If `any` is specified, the destination IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the target IPv4 address.

If own-prefix is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where own-address and own-prefix are specified is multihomed, the primary IPv4 address is the target.

If range-address is specified, the flow detection condition is in the range from <*destination ipv4 start*> to <*destination ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv4 address for <*destination ipv4*>.

   For <*destination ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*destination ipv4 end*> is larger than <*destination ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If eq is specified, the flow detection condition is an exact match of <*destination port*>.

If neq is specified, the flow detection condition is other than <*destination port*>.

If range is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-5: Port names that can be specified for UDP (IPv4)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

tos <*tos*>

Specifies 4 bits (bits 3 to 6) in the ToS field as the tos value.

The TOS value is compared with 4 bits (bits 3 to 6) in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 2-7: tos names that can be specified*.

precedence <*precedence*>

Specifies the precedence value, which is the first 3 bits in the ToS field.

Its value is compared with the first 3 bits in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 2-8: precedence names that can be specified*.

dscp <*dscp*>

Specifies the DSCP value, which is the first 6 bits in the ToS field.

Its value is compared with the first 6 bits in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 2-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

None

<icmp type>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp code>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp message>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be specified, see *Table 2-12: Message names that can be specified for ICMP (IPv4)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<igmp type>

Specifies the IGMP type.

This parameter option is available only if the protocol is IGMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

length {upper | lower} *<length>*

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of *<length>* or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of *<length>* or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

Specifies the MF flag value, which is the lower 1 bit in the Flags field.

`+mf` indicates a packet where an MF flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an MF flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `255.255.255.255` is entered for the source address wildcard mask and the destination address wildcard mask, `any` is displayed.
2. If `0.0.0.0` is entered for the source address wildcard mask and the destination address wildcard mask, `host` *nnn.nnn.nnn.nnn*, `host own-address` is displayed.

Related commands

```
ip access-group
ip access-list resequence
permit (ip access-list extended)
remark
```

deny (ip access-list standard)

Specifies the conditions by which the IPv4 address filter denies access.

Syntax

To set or change information:

```
[<sequence>] deny {<ipv4> [<ipv4 wildcard>] | host <ipv4> | any}
```

To delete information:

```
no <sequence>
```

Input mode

```
(config-std-nacl)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{<*ipv4*> [<*ipv4 wildcard*>] | host <*ipv4*> | any}

Specify an IPv4 address.

If host <*ipv4*> is specified, the flow detection condition is an exact match of <*ipv4*>.

To specify all IPv4 addresses, specify `any`. If `any` is specified, the IPv4 address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*ipv4*>, specify an address in IPv4 format.

   For [<*ipv4 wildcard*>], specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary. If wildcards are omitted, the filter condition is an exact match of <*ipv4*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `255.255.255.255` is entered as the address wildcard mask, `any` is displayed.
2. If `0.0.0.0` is entered as the address wildcard mask, `host` *nnn.nnn.nnn.nnn* is displayed.

Related commands

```
ip access-group
ip access-list resequence
permit (ip access-list standard)
remark
```

deny (ipv6 access-list)

Specifies the conditions by which the IPv6 filter denies access.

If the `+fo` parameter is set for the flow detection conditions, the VLAN tag header conditions and IPv6 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

Syntax

To set or change information:

```
[<sequence>] deny <target flow>
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, and ICMP:

```
{ipv6 | <protocol>} {<source ipv6>/<length> | host {<source ipv6> |
own-address} | any | own-address <own address length>} {<destination ipv6>/
<length>| host {<destination ipv6> | own-address} | any | own-address <own
address length> | own-prefix | range-address <destination ipv6 start>
<destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged |
user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
tcp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} [{{eq | neq} <source port> | range <source
port start> <source port end>}] {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{{eq | neq} <destination port> | range <destination port start> <destination
port end>}] [{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}]
[{+rst | -rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{traffic-class <traffic
class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo]
[{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is UDP:

```
udp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} [{{eq | neq} <source port> | range <source
port start> <source port end>}] {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{{eq | neq}<destination port> | range <destination port start> <destination
port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is ICMP:

```
icmp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic
class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo]
[{untagged | user-priority <priority>}]
```

When the `+fo` parameter is specified:

```
{ipv6 | <protocol> | icmp | tcp | udp} {<source ipv6>/<length> | host {<source
ipv6> | own-address} | any | own-address <own address length>} {<destination
ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address
<own address length> | own-prefix | range-address <destination ipv6 start>
<destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
user-priority <priority>}]
```

Input mode

```
(config-ipv6-acl)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{ipv6 | *<protocol>* | icmp | tcp | udp}

Specifies the upper-layer protocol condition for IPv6 packets. Note that if all protocols are applicable, specify `ipv6`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 42, 45 to 49, 52 to 59, 61 to 255 (in decimal), or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-3: Protocol names that can be specified (IPv6)*.

{*<source ipv6>*/*<length>* | host {*<source ipv6>* | own-address} | any | own-address *<own address length>*}

Specifies the source IPv6 address.

If `host` *<source ipv6>* is specified, the flow detection condition is an exact match of *<source ipv6>*.

To specify all source IPv6 addresses, specify `any`. If `any` is specified, the source IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the source IPv4 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv6 address for *<source ipv6>*.

   For *<length>*, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

<*source ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<*length*>: 0 to 128

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-6: Port names that can be specified for UDP (IPv6).*

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

If `host` <*destination ipv6*> is specified, the flow detection condition is an exact match of <*destination ipv6*>.

To specify all destination IPv6 addresses, specify `any`. If `any` is specified, the destination IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the target IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the target IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv6 start*> to <*destination ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv6 address for <*destination ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

Specify IPv6 addresses so that <*destination ipv6 end*> is larger than <*destination ipv6 start*>.

<*destination ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<*length*>: 0 to 128

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*destination port*>.

If `neq` is specified, the flow detection condition is other than <*destination port*>.

If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

traffic-class <*traffic class*>

Specifies the traffic class field value.

Its value is compared with the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

dscp <*dscp*>

Specifies the DSCP value, which is the first 6 bits in the traffic class field.

Its value is compared with the first 6 bits in the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 2-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<*icmp type*>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<*icmp code*>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<*icmp message*>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be specified, see *Table 2-13: Message names that can be specified for ICMP (IPv6)*.

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

length {upper | lower} <*length*>

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of <*length*> or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of <*length*> or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

Specifies the M flag value of the fragment header.

`+mf` indicates a packet where an M flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an M flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority.

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If 0 is entered for the <*length*> or <*own address length*> of the source address and destination address, `any` is displayed.
2. If 128 is entered for the <*length*> or <*own address length*> of the source address and destination address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*, `host own-address` is displayed.

Related commands

```
ipv6 traffic-filter
ipv6 access-list resequence
permit (ipv6 access-list)
remark
```

deny (mac access-list extended)

Specifies the conditions by which the MAC filter denies access.

Syntax

To set or change information:

```
[<sequence>] deny <target flow>
```

To delete information:

```
no <sequence>
```

■ *<target flow>*:

```
{<source mac> <source mac mask> | host <source mac> | any} {<destination mac>
<destination mac mask> | host <destination mac> | any | <destination mac name>}
[<ethernet type>] [{untagged | [user-priority <priority>] [tag-vlan <vlan id>]}]
```

Input mode

```
(config-ext-macl)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{*<source mac>* *<source mac mask>* | host *<source mac>* | any}

Specifies the source MAC address.

If `host` *<source mac>* is specified, the flow detection condition is an exact match of *<source mac>*.

To specify all source MAC addresses, specify `any`. If `any` is specified, the source MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source MAC address for *<source mac>*.

   For *<source mac mask>*, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{*<destination mac>* *<destination mac mask>* | host *<destination mac>* | any | *<destination*

mac name>}

Specifies the destination MAC address.

If `host` *<destination mac>* is specified, the flow detection condition is an exact match of *<destination mac>*.

To specify all destination MAC addresses, specify `any`. If `any` is specified, the destination MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination MAC address for *<destination mac>*.

   For *<destination mac mask>*, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   Specify the destination MAC address for *<destination mac name>*. For details about the destination MAC address names that can be specified, see *Table 2-11: Destination MAC address names that can be specified*.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<ethernet type>

Specifies the Ethernet type value.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name.

   For details about the Ethernet type names that can be specified, see *Table 2-10: Ethernet type names that can be specified*.

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority *<priority>*

Specifies the user priority of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

tag-vlan *<vlan id>*

Specifies the VLAN ID of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 4095 in decimal.

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If *nnnn.nnnn.nnnn* `ffff.ffff.ffff` is entered as the source address and the destination address, `any` is displayed.
2. If the destination MAC address name or the address of the destination MAC address name is entered for the destination MAC address, the destination MAC address name is displayed.

   If *nnnn.nnnn.nnnn* `0000.0000.0000` is entered as the source address and the destination address in cases other than the above, `host` *nnnn.nnnn.nnnn* is displayed.

Related commands

```
mac access-group
mac access-list resequence
permit (mac access-list extended)
remark
```

ip access-group

Applies an IPv4 access list to an interface, and enables the IPv4 filtering functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

If you apply an access list with the policy-based routing parameter specified, specify the inbound (receiving) side.

Syntax

To set information:

```
ip access-group <access list name> {in | out}
```

To delete information:

```
no ip access-group <access list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<access list name>

Specify the access list name of the IPv4 address filter or the IPv4 packet filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

When an access list with at least one entry is removed from an interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One can be set for each inbound and outbound side of the same interface. If it is already set, delete before specifying the setting.
2. If you specify a non-existent IPv4 filter, no action is performed. The access list name of the IPv4 filter is registered.
3. This can be set if an IPv4 address is set for the target interface when there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
4. If policy-based routing is specified, the IPv4 address that is set for the target interface cannot be set for the destination IPv4 address of the flow detection conditions.

Related commands

```
ip access-list standard
ip access-list extended
```

ip access-list extended

Sets an access list used as an IPv4 filter. There are two types of access lists that operate as IPv4 filters. One type is an IPv4 address filter and the other type is an IPv4 packet filter.

This command sets an IPv4 packet filter. After this command is executed, the mode changes to `config-ext-nacl` mode.

Syntax

To set information:

```
    ip access-list extended <access list name>
```

To delete information:

```
    no ip access-list extended <access list name>
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the access list name of the IPv4 packet filter.

Access list names that are already being used in the IPv4 address filter, IPv6 filter, MAC filter, and Advance filter cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

When an access list with at least one entry that was already applied to an interface is removed from the interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ip access-group
ip access-list resequence
deny (ip access-list extended)
permit (ip access-list extended)
remark
```

ip access-list resequence

Re-sequences the sequence numbers that determine the order in which the IPv4 address filter and IPv4 packet filter apply flow detection conditions.

Syntax

To set or change information:

```
ip access-list resequence <access list name> [<starting sequence> [<increment
sequence>]]
```

Input mode

```
(config)
```

Parameters

<access list name>

Specify the access list name of the IPv4 address filter or the IPv4 packet filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ip access-list standard
ip access-list extended
```

ip access-list standard

Sets an access list to be used as an IPv4 filter. There are two types of access lists that operate as IPv4 filters. One type is an IPv4 address filter and the other type is an IPv4 packet filter.

This command sets an IPv4 address filter. After this command is executed, the mode changes to `config-std-nacl` mode.

Syntax

To set information:

```
ip access-list standard <access list name>
```

To delete information:

```
no ip access-list standard <access list name>
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the access list name of the IPv4 address filter.

Access list names that are already being used in the IPv4 packet filter, IPv6 filter, MAC filter, and Advance filter cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

When an access list with at least one entry that was already applied to an interface is removed from the interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ip access-group
ip access-list resequence
deny (ip access-list standard)
permit (ip access-list standard)
remark
```

ipv6 access-list

Configures an access list to serve as an IPv6 filter. After this command is executed, the mode changes to `config-ipv6-acl` mode.

Syntax

To set information:

```
ipv6 access-list <access list name>
```

To delete information:

```
no ipv6 access-list <access list name>
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the access list name of the IPv6 filter.

Access list names that are already being used in the IPv4 address filter, IPv4 packet filter, MAC filter, and Advance filter cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

When an access list with at least one entry that was already applied to an interface is removed from the interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ipv6 traffic-filter
ipv6 access-list resequence
deny (ipv6 access-list)
permit (ipv6 access-list)
remark
```

ipv6 access-list resequence

Re-sequences the sequence numbers that determine the order in which the IPv6 filter applies flow detection conditions.

Syntax

To set or change information:

```
    ipv6 access-list resequence <access list name> [<starting sequence>
    [<increment sequence>]]
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the access list name of the IPv6 filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ipv6 access-list
```

ipv6 traffic-filter

Applies an IPv6 access list to an interface, and enables the IPv6 filtering functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

If you apply an access list with the policy-based routing parameter specified, specify the inbound (receiving) side.

Syntax

To set information:

```
ipv6 traffic-filter <access list name> {in | out}
```

To delete information:

```
no ipv6 traffic-filter <access list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<access list name>

Specifies the access list name of the IPv6 filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

When an access list with at least one entry is removed from an interface, the IPv6 packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One can be set for each inbound and outbound side of the same interface. If it is already set, delete before specifying the setting.
2. If you specify a non-existent IPv6 filter, no action is performed. The access list name of the IPv6 filter is registered.
3. This can be set if a single IPv6 global address only is set for the target interface when there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
4. This can be set if `any` or <*length*> of 64 or less is specified for the source address of the flow detection conditions parameter.
5. If policy-based routing is specified, the IPv6 global address that is set for the target interface cannot be set for the destination IPv6 address of the flow detection conditions.

Related commands

```
ipv6 access-list
```

mac access-group

Applies a MAC access list to an interface, and enables the MAC filtering functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

Syntax

To set information:

```
mac access-group <access list name> {in | out}
```

To delete information:

```
no mac access-group <access list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<access list name>

Specifies the access list name of the MAC filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

When an access list with at least one entry is removed from an interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One can be set for each inbound and outbound side of the MAC filter. If it is already set, delete before specifying the setting.
2. If you specify a non-existent MAC filter, no action is performed. The access list name of the MAC filter is registered.

Related commands

```
mac access-list extended
```

mac access-list extended

Sets an access list to be used in a MAC filter. After this command is executed, the mode changes to `config-ext-macl` mode.

Syntax

To set information:

```
mac access-list extended <access list name>
```

To delete information:

```
no mac access-list extended <access list name>
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the access list name of the MAC filter.

Access list names that are already being used in the IPv4 address filter, IPv4 packet filter, IPv6 filter, and Advance filter cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

When an access list with at least one entry that was already applied to an interface is removed from the interface, the packets received at the relevant interface are discarded temporarily until all entries are removed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
mac access-group
mac access-list resequence
deny (mac access-list extended)
permit (mac access-list extended)
remark
```

mac access-list resequence

Re-sequences the sequence numbers that determine the order in which the MAC filter applies flow detection conditions.

Syntax

To set or change information:

```
mac access-list resequence <access list name> [<starting sequence>
[<increment sequence>]]
```

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the access list name of the MAC filter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
        mac access-list extended
```

permit (advance access-list)

Specifies the conditions by which the Advance filter permits access.

Syntax

To set or change information:

```
[<sequence>] permit mac <target flow>
[<sequence>] permit mac-ip <target flow> [<action specification>]
[<sequence>] permit mac-ipv6 <target flow> [<action specification>]
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

For `mac` *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions.

```
mac {<source mac> <source mac mask> | host <source mac> | any} {<destination
mac> <destination mac mask> | host <destination mac> | any | <destination mac
name>} [<ethernet type>] [{untagged | [user-priority <priority>] [tag-vlan
<vlan id>]}]
```

For `mac-ip` *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions, VLAN Tag header conditions, IPv4 header conditions, or Layer 4 header conditions.

If the `+fo` parameter is set for the flow detection conditions, the MAC header conditions, VLAN tag header conditions, and IPv4 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, ICMP, and IGMP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ip | <protocol>} {{<source ipv4> |
own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address}
| any | own-prefix | range-address <source ipv4 start> <source ipv4 end>}
{{<destination ipv4> | own-address} <destination ipv4 wildcard> | host
{<destination ipv4> | own-address} | any | own-prefix | range-address
<destination ipv4 start> <destination ipv4 end>} [{[tos <tos>]
[precedence <precedence>] | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} tcp {{<source ipv4> | own-address} <source ipv4
wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source
port> | range <source port start> <source port end>}] {{<destination
ipv4> | own-address} <destination ipv4 wildcard> | host {<destination
ipv4> | own-address} | any | own-prefix | range-address <destination ipv4
start> <destination ipv4 end>} [{{eq | neq} <destination port> | range
<destination port start> <destination port end>}] [{[established] |
[{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}] [{+rst | -rst}] [{+syn |
-syn}] [{+urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp
<dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged
| [user-priority <priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is UDP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} udp {{<source ipv4> | own-address} <source ipv4
wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source
port> | range <source port start> <source port end>}] {{<destination
ipv4> | own-address} <destination ipv4 wildcard> | host {<destination
ipv4> | own-address} | any | own-prefix | range-address <destination ipv4
start> <destination ipv4 end>} [{{eq | neq} <destination port> | range
<destination port start> <destination port end>}] [{[tos <tos>]
[precedence <precedence>] | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is ICMP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} icmp {{<source ipv4> | own-address} <source
ipv4 wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4>
| own-address} <destination ipv4 wildcard> | host {<destination ipv4> |
own-address} | any | own-prefix | range-address <destination ipv4 start>
<destination ipv4 end>} [{<icmp type> [<icmp code>] | <icmp message>}]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority
<priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is IGMP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} igmp {{<source ipv4> | own-address} <source
ipv4 wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4>
| own-address} <destination ipv4 wildcard> | host {<destination ipv4> |
own-address} | any | own-prefix | range-address <destination ipv4 start>
<destination ipv4 end>} [<igmp type>] [{[tos <tos>] [precedence
<precedence>] | dscp <dscp>}] [length {upper | lower} <length>] [{+mf |
-mf}] [-fo] [{untagged | [user-priority <priority>] [tag-vlan <vlan
id>]}]
```

When the +fo parameter is specified:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ip | <protocol> | icmp | igmp | tcp | udp}
{{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4
start> <source ipv4 end>} {{<destination ipv4> | own-address}
<destination ipv4 wildcard> | host {<destination ipv4> | own-address} |
any | own-prefix | range-address <destination ipv4 start> <destination
ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
[user-priority <priority>] [tag-vlan <vlan id>]}]
```

For mac-ipv6 *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions, VLAN Tag header conditions, IPv6 header conditions, or Layer 4 header conditions.

If the +fo parameter is set for the flow detection conditions, the MAC header conditions, VLAN tag header conditions, and IPv6 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

When the +fo parameter is not specified and the upper layer protocol is a type other than TCP, UDP, and ICMP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ipv6 | <protocol>} {<source ipv6>/<length>|
host {<source ipv6> | own-address} | any | own-address <own address
length> | own-prefix | range-address <source ipv6 start> <source ipv6
end>} {<destination ipv6>/<length>| host {<destination ipv6> |
own-address} | any | own-address <own address length> | own-prefix |
range-address <destination ipv6 start> <destination ipv6 end>}
[{traffic-class <traffic class> | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is TCP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} tcp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any| own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq}
<source port> | range <source port start> <source port end>}]
{<destination ipv6>/<length>| host {<destination ipv6> | own-address} |
any | own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port
end>}] [{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}]
[{+rst | -rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{traffic-class
<traffic class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf
| -mf}] [-fo] [{untagged | [user-priority <priority>] [tag-vlan <vlan
id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is UDP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} udp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any | own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq}
<source port> | range <source port start> <source port end>}]
{<destination ipv6>/<length>| host {<destination ipv6> | own-address} |
any | own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port
end>}] [{traffic-class <traffic class> | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority
<priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is ICMP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} icmp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any | own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} {<destination
ipv6>/<length>| host {<destination ipv6> | own-address} | any |
own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp
code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged |
[user-priority <priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is specified:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ipv6 | <protocol> | icmp | tcp | udp} {<source
ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address
<own address length> | own-prefix | range-address <source ipv6 start>
<source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6>
| own-address} | any | own-address <own address length> | own-prefix |
range-address <destination ipv6 start> <destination ipv6 end>}
[{traffic-class <traffic class> | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [+fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

- *<action specification>*:

For `mac-ip` *<target flow>* `[`*<action specification>*`]` or `mac-ipv6` *<target flow>* `[`*<action specification>*`]`:

```
action policy-list <policy list name>
```

Input mode

```
(config-adv-acl)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{*<source mac>* *<source mac mask>* | host *<source mac>* | any}

Specifies the source MAC address.

If `host` *<source mac>* is specified, the flow detection condition is an exact match of *<source mac>*.

To specify all source MAC addresses, specify `any`. If `any` is specified, the source MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source MAC address for *<source mac>*.

   For *<source mac mask>*, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{*<destination mac>* *<destination mac mask>* | host *<destination mac>* | any | *<destination mac name>*}

Specifies the destination MAC address.

If `host` *<destination mac>* is specified, the flow detection condition is an exact match of *<destination mac>*.

To specify all destination MAC addresses, specify `any`. If `any` is specified, the destination MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination MAC address for <*destination mac*>.

   For <*destination mac mask*>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   Specify the destination MAC address for <*destination mac name*>. For details about the destination MAC address names that can be specified, see *Table 2-11: Destination MAC address names that can be specified*.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<*ethernet type*>

Specifies the Ethernet type value.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name.

   For details about the Ethernet type names that can be specified, see *Table 2-10: Ethernet type names that can be specified*.

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

tag-vlan <*vlan id*>

Specifies the VLAN ID of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 4095 in decimal.

{ip | <*protocol*> | icmp | igmp | tcp | udp}

You can select this parameter when `mac-ip` is specified as the flow detection condition.

Specifies the upper-layer protocol condition for IPv4 packets. Note that if all protocols are applicable, specify `ip`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set 0 to 255 (in decimal) or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-2: Protocol names that can be specified (IPv4)*.

{ipv6 | <*protocol*> | icmp | tcp | udp}

You can select this parameter if `mac-ipv6` is specified as the flow detection condition.

Specifies the upper-layer protocol condition for IPv6 packets. Note that if all protocols are applicable, specify `ipv6`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 42, 45 to 49, 52 to 59, 61 to 255 (in decimal), or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-3: Protocol names that can be specified (IPv6)*.

{{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>}

Specifies the source IPv4 address.

If `host` <*source ipv4*> is specified, the flow detection condition is an exact match of <*source ipv4*>.

To specify all source IPv4 addresses, specify `any`. If `any` is specified, the source IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the source IPv4 address.

If own-prefix is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*source ipv4 start*> to <*source ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv4 address for <*source ipv4*>.

   For <*source ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*source ipv4 end*> is larger than <*source ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*source ipv6 start*> <*source ipv6 end*>}

Specifies the source IPv6 address.

If `host` <*source ipv6*> is specified, the flow detection condition is an exact match of <*source ipv6*>.

To specify all source IPv6 addresses, specify `any`. If `any` is specified, the source IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the source IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the source IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*source ipv6 start*> to <*source ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv6 address for <*source ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

   Specify IPv6 addresses so that <*source ipv6 end*> is larger than <*source ipv6 start*>.

   <*source ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <*length*>: 0 to 128

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be specified, see *Table 2-4: Port names that can be specified for TCP*, *Table 2-5: Port names that can be specified for UDP (IPv4)*, or *Table 2-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

If `host` <*destination ipv4*> is specified, the flow detection condition is an exact match of <*destination ipv4*>.

To specify all destination IPv4 addresses, specify `any`. If `any` is specified, the destination IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the target IPv4 address.

If `own-prefix` is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv4 start*> to <*destination ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv4 address for <*destination ipv4*>.

   For <*destination ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*destination ipv4 end*> is larger than <*destination ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

If `host` <*destination ipv6*> is specified, the flow detection condition is an exact match of <*destination ipv6*>.

To specify all destination IPv6 addresses, specify `any`. If `any` is specified, the destination IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the target IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the target IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv6 start*> to <*destination ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Specify the destination IPv6 address for <*destination ipv6*>.

For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

Specify IPv6 addresses so that <*destination ipv6 end*> is larger than <*destination ipv6 start*>.

<*destination ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<*length*>: 0 to 128

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*destination port*>.

If `neq` is specified, the flow detection condition is other than <*destination port*>.

If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be specified, see *Table 2-4: Port names that can be specified for TCP*, *Table 2-5: Port names that can be specified for UDP (IPv4)*, or *Table 2-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

tos <*tos*>

Specifies 4 bits (bits 3 to 6) in the ToS field as the tos value.

The TOS value is compared with 4 bits (bits 3 to 6) in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 2-7: tos names that can be specified*.

precedence <*precedence*>

Specifies the precedence value, which is the first 3 bits in the ToS field.

Its value is compared with the first 3 bits in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 2-8: precedence names that can be specified*.

traffic-class <*traffic class*>

Specifies the traffic class field value.

Its value is compared with the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

dscp <*dscp*>

- When the flow detection condition type is `mac-ip`:

  Specifies the DSCP value, which is the first 6 bits in the ToS field.

  Its value is compared with the first 6 bits in the ToS field of the received packet.

- When the flow detection condition type is `mac-ipv6`:

  Specifies the DSCP value, which is the first 6 bits in the traffic class field.

  Its value is compared with the first 6 bits in the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 2-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<icmp type>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp code>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp message>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be set, see *Table 2-12: Message names that can be specified for ICMP (IPv4)* or *Table 2-13: Message names that can be specified for ICMP (IPv6)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<igmp type>

Specifies the IGMP type.

This parameter option is available only if the protocol is IGMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

length {upper | lower} <*length*>

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of <*length*> or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of <*length*> or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

- When the flow detection condition type is `mac-ip`:

  Specifies the MF flag value, which is the lower 1 bit in the Flags field.

  `+mf` indicates a packet where an MF flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an MF flag of 0 is set for the flow detection conditions.

- When the flow detection condition type is `mac-ipv6`:

  Specifies the M flag value of the fragment header.

  `+mf` indicates a packet where an M flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an M flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<*action specification*> parameter

action

Specifies the operation of the packet where a flow was detected. Specify the start of the entire <*action specification*> parameter.

1. Default value when this parameter is omitted:

   None (No operation is specified.)

2. Range of values:

None

policy-list <*policy list name*>

Specifies the policy-based routing list name.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   If the flow detection condition type is `mac-ip`, this specifies the policy-based routing list name that was set by the `ip policy-list` command.

   If the flow detection condition type is `mac-ipv6`, this specifies the policy-based routing list name that was set by the `ipv6 policy-list` command.

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If *nnnn*.*nnnn*.*nnnn* `ffff.ffff.ffff` is entered as the source MAC address and the destination MAC address, `any` is displayed.
2. If the destination MAC address name or the address of the destination MAC address name is entered for the destination MAC address, the destination MAC address name is displayed.

   If *nnnn*.*nnnn*.*nnnn* `0000.0000.0000` is entered as the source MAC address and the destination MAC address in cases other than the above, `host` *nnnn.nnnn.nnnn* is displayed.
3. If `255.255.255.255` is entered for the source IPv4 address wildcard mask and the destination IPv4 address wildcard mask, `any` is displayed.
4. If `0.0.0.0` is entered for the source IPv4 address wildcard mask and the destination IPv4 address wildcard mask, `host` *nnn*.*nnn*.*nnn*.*nnn*, `host own-address` is displayed.
5. If 0 is entered for the <*length*> or <*own address length*> of the source IPv6 address and destination IPv6 address, `any` is displayed.
6. If 128 is entered for the <*length*> or <*own address length*> of the source IPv6 address and destination IPv6 address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*, `host own-address` is displayed.
7. If policy-based routing is specified, the following addresses cannot be specified for the source IPv4 address and destination IPv4 address that are specified for the flow detection conditions:

   Source IPv4 address

   Multicast addresses

   Destination IPv4 address

   Multicast address, restricted broadcast address, and `host own-address` parameter
8. If policy-based routing is specified, the following addresses cannot be specified for the source IPv6 address and destination IPv6 address that are specified for the flow detection conditions:

   Source IPv6 address

Multicast address and link-local address

Destination IPv6 address

Multicast address, link-local address, and `host own-address` parameter

Related commands

```
advance access-group
advance access-list resequence
deny (advance access-list)
remark
ip policy-list
ipv6 policy-list
```

permit (ip access-list extended)

Specifies the conditions by which the IPv4 packet filter permits access.

If the `+fo` parameter is set for the flow detection conditions, the VLAN tag header conditions and IPv4 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

Syntax

To set or change information:

```
[<sequence>] permit <target flow> [<action specification>]
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, ICMP, and IGMP:

```
{ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> |
host {<source ipv4> | own-address} | any | own-prefix | range-address <source
ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address}
<destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any
| own-prefix | range-address <destination ipv4 start> <destination ipv4 end>}
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} [{{eq | neq} <source port> | range <source port start>
<source port end>}] {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port end>}]
[{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}] [{+rst |
-rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{[tos <tos>] [precedence
<precedence>] | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}]
[-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is UDP:

```
udp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} [{{eq | neq} <source port> | range <source port start>
<source port end>}] {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port end>}]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is ICMP:

```
icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{<icmp type>
[<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] |
dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged
| user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is IGMP:

```
igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is specified:

```
{ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address}
<source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own-prefix
| range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4>
| own-address} <destination ipv4 wildcard> | host {<destination ipv4> |
own-address} | any | own-prefix | range-address <destination ipv4 start>
<destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp
<dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
user-priority <priority>}]
```

- <*action specification*>:
  `action policy-list <policy list name>`

Input mode

`(config-ext-nacl)`

Parameters

<*sequence*>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<*target flow*> parameter

{ip | <*protocol*> | icmp | igmp | tcp | udp}

Specifies the upper-layer protocol condition for IPv4 packets. Note that if all protocols are applicable, specify `ip`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set 0 to 255 (in decimal) or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-2: Protocol names that can be specified (IPv4).*

{{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>}

Specifies the source IPv4 address.

If `host` <*source ipv4*> is specified, the flow detection condition is an exact match of <*source ipv4*>.

To specify all source IPv4 addresses, specify `any`. If `any` is specified, the source IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the source IPv4 address.

If own-prefix is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*source ipv4 start*> to <*source ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv4 address for <*source ipv4*>.

   For <*source ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*source ipv4 end*> is larger than <*source ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-5: Port names that can be specified for UDP (IPv4)*.

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

If `host` <*destination ipv4*> is specified, the flow detection condition is an exact match of <*destination ipv4*>.

To specify all destination IPv4 addresses, specify `any`. If `any` is specified, the destination IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the target IPv4 address.

If `own-prefix` is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv4 start*> to <*destination ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv4 address for <*destination ipv4*>.

   For <*destination ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*destination ipv4 end*> is larger than <*destination ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*destination port*>.

If `neq` is specified, the flow detection condition is other than <*destination port*>.

If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-5: Port names that can be specified for UDP (IPv4)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

tos <*tos*>

Specifies 4 bits (bits 3 to 6) in the ToS field as the tos value.

The TOS value is compared with 4 bits (bits 3 to 6) in the ToS field of the sent or received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 15 (in decimal) or a tos name.

For details about the tos names that can be specified, see *Table 2-7: tos names that can be specified*.

precedence <*precedence*>

Specifies the precedence value, which is the first 3 bits in the ToS field.

Its value is compared with the first 3 bits in the ToS field of the sent or received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 2-8: precedence names that can be specified*.

dscp <*dscp*>

Specifies the DSCP value, which is the first 6 bits in the ToS field.

Its value is compared with the first 6 bits in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 2-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<icmp type>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp code>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp message>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be specified, see *Table 2-12: Message names that can be specified for ICMP (IPv4)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<igmp type>

Specifies the IGMP type.

This parameter option is available only if the protocol is IGMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

length {upper | lower} *<length>*

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of *<length>* or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of *<length>* or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

Specifies the MF flag value, which is the lower 1 bit in the Flags field.

`+mf` indicates a packet where an MF flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an MF flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

<*action specification*> parameter

action

Specifies the operation of the packet where a flow was detected. Specify the start of the entire <*action specification*> parameter.

1. Default value when this parameter is omitted:

   None (No operation is specified.)

2. Range of values:

   None

policy-list <*policy list name*>

Specifies the policy-based routing list name.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   Specifies the policy-based routing list name that was set by using the `ip policy-list` command.

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `255.255.255.255` is entered for the source address wildcard mask and the destination address wildcard mask, `any` is displayed.
2. If `0.0.0.0` is entered for the source address wildcard mask and the destination address wildcard mask, `host` *nnn.nnn.nnn.nnn*, `host own-address` is displayed.
3. If policy-based routing is specified, the following addresses cannot be specified for the source IPv4 address and destination IPv4 address that are specified for the flow detection conditions:

   Source IPv4 address

   Multicast addresses

   Destination IPv4 address

   Multicast address, restricted broadcast address, and `host own-address` parameter

Related commands

```
ip access-group
ip access-list resequence
deny (ip access-list extended)
remark
ip policy-list
```

permit (ip access-list standard)

Specifies the conditions by which the IPv4 address filter permits access.

Syntax

To set or change information:

```
[<sequence>] permit {<ipv4> [<ipv4 wildcard>] | host <ipv4> | any}
```

To delete information:

```
no <sequence>
```

Input mode

```
(config-std-nacl)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{<*ipv4*> [<*ipv4 wildcard*>] | host <*ipv4*> | any}

Specify an IPv4 address.

If host <*ipv4*> is specified, the flow detection condition is an exact match of <*ipv4*>.

To specify all IPv4 addresses, specify `any`. If `any` is specified, the IPv4 address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*ipv4*>, specify an address in IPv4 format.

   For [<*ipv4 wildcard*>], specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary. If wildcards are omitted, the filter condition is an exact match of <*ipv4*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `255.255.255.255` is entered as the address wildcard mask, `any` is displayed.
2. If `0.0.0.0` is entered as the address wildcard mask, `host` *nnn.nnn.nnn.nnn* is displayed.

Related commands

```
ip access-group
ip access-list resequence
deny (ip access-list standard)
remark
```

permit (ipv6 access-list)

Specifies the conditions by which the IPv6 filter permits access.

If the `+fo` parameter is set for the flow detection conditions, the VLAN tag header conditions and IPv6 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

Syntax

To set or change information:

```
[<sequence>] permit <target flow> [<action specification>]
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, and ICMP:

```
{ipv6 | <protocol>} {<source ipv6>/<length> | host {<source ipv6> |
own-address} | any | own-address <own address length>} {<destination ipv6>/
<length>| host {<destination ipv6> | own-address} | any | own-address <own
address length> | own-prefix | range-address <destination ipv6 start>
<destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged |
user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
tcp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} [{{eq | neq} <source port> | range <source
port start> <source port end>}] {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{{eq | neq} <destination port> | range <destination port start> <destination
port end>}] [{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}]
[{+rst | -rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{traffic-class <traffic
class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo]
[{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is UDP:

```
udp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} [{{eq | neq} <source port> | range <source
port start> <source port end>}] {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{{eq | neq}<destination port> | range <destination port start> <destination
port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is ICMP:

```
icmp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic
class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo]
[{untagged | user-priority <priority>}]
```

When the `+fo` parameter is specified:

```
{ipv6 | <protocol> | icmp | tcp | udp} {<source ipv6>/<length> | host {<source
ipv6> | own-address} | any | own-address <own address length>} {<destination
ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address
<own address length> | own-prefix | range-address <destination ipv6 start>
<destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
user-priority <priority>}]
```

- *<action specification>*:
  `action policy-list <policy list name>`

Input mode

`(config-ipv6-acl)`

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{ipv6 | *<protocol>* | icmp | tcp | udp}

Specifies the upper-layer protocol condition for IPv6 packets. Note that if all protocols are applicable, specify `ipv6`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 42, 45 to 49, 52 to 59, 61 to 255 (in decimal), or a protocol name.

   For details about the protocol names that can be specified, see *Table 2-3: Protocol names that can be specified (IPv6).*

{*<source ipv6>*/*<length>* | host {*<source ipv6>* | own-address} | any | own-address *<own address length>*}

Specifies the source IPv6 address.

If `host` *<source ipv6>* is specified, the flow detection condition is an exact match of *<source ipv6>*.

To specify all source IPv6 addresses, specify `any`. If `any` is specified, the source IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the source IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv6 address for *<source ipv6>*.

For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

For <*own address length*>, specify the part of `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

<*source ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<*length*>: 0 to 128

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

If `host` <*destination ipv6*> is specified, the flow detection condition is an exact match of <*destination ipv6*>.

To specify all destination IPv6 addresses, specify `any`. If `any` is specified, the destination IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the target IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the target IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv6 start*> to <*destination ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv6 address for <*destination ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

Specify IPv6 addresses so that <*destination ipv6 end*> is larger than <*destination ipv6 start*>.

<*destination ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<*length*>: 0 to 128

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*destination port*>.

If `neq` is specified, the flow detection condition is other than <*destination port*>.

If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 2-4: Port names that can be specified for TCP* or *Table 2-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

traffic-class <*traffic class*>

Specifies the traffic class field value.

Its value is compared with the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

dscp <*dscp*>

Specifies the DSCP value, which is the first 6 bits in the traffic class field.

Its value is compared with the first 6 bits in the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 2-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<icmp type>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp code>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp message>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be specified, see *Table 2-13: Message names that can be specified for ICMP (IPv6)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

length {upper | lower} <*length*>

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of <*length*> or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of <*length*> or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

Specifies the M flag value of the fragment header.

`+mf` indicates a packet where an M flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an M flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

<*action specification*> parameter

action

Specifies the operation of the packet where a flow was detected. Specify the start of the entire <*action specification*> parameter.

1. Default value when this parameter is omitted:

   None (No operation is specified.)

2. Range of values:

   None

policy-list <*policy list name*>

Specifies the policy-based routing list name.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   Specifies the policy-based routing list name that was set by using the `ipv6 policy-list` command.

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If 0 is entered for the <*length*> or <*own address length*> of the source address and destination address, `any` is displayed.
2. If 128 is entered for the <*length*> or <*own address length*> of the source address and destination address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*, `host own-address` is displayed.
3. If policy-based routing is specified, the following addresses cannot be specified for the source IPv6 address and destination IPv6 address that are specified for the flow detection conditions:

   Source IPv6 address

   Multicast address and link-local address

   Destination IPv6 address

   Multicast address, link-local address, and `host own-address` parameter

Related commands

```
ipv6 traffic-filter
ipv6 access-list resequence
deny (ipv6 access-list)
remark
ipv6 policy-list
```

permit (mac access-list extended)

Specifies the conditions by which the MAC filter permits access.

Syntax

To set or change information:

```
[<sequence>] permit <target flow>
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

```
{<source mac> <source mac mask> | host <source mac> | any} {<destination mac>
<destination mac mask> | host <destination mac> | any | <destination mac name>}
[<ethernet type>] [{untagged | [user-priority <priority>] [tag-vlan <vlan id>]}]
```

Input mode

```
(config-ext-macl)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{*<source mac>* *<source mac mask>* | host *<source mac>* | any}

Specifies the source MAC address.

If host *<source mac>* is specified, the flow detection condition is an exact match of *<source mac>*.

To specify all source MAC addresses, specify `any`. If `any` is specified, the source MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source MAC address for *<source mac>*.

   For *<source mac mask>*, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{*<destination mac>* *<destination mac mask>* | host *<destination mac>* | any | *<destination*

mac name>}

Specifies the destination MAC address.

If host <*destination mac*> is specified, the flow detection condition is an exact match of <*destination mac*>.

To specify all destination MAC addresses, specify `any`. If `any` is specified, the destination MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination MAC address for <*destination mac*>.

   For <*destination mac mask*>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   Specify the destination MAC address for <*destination mac name*>. For details about the destination MAC address names that can be specified, see *Table 2-11: Destination MAC address names that can be specified*.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<*ethernet type*>

Specifies the Ethernet type value.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name. For details about the Ethernet type names that can be specified, see *Table 2-10: Ethernet type names that can be specified*.

untagged

Specifies the detection of Untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

tag-vlan <*vlan id*>

Specifies the VLAN ID of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 4095 in decimal.

Default behavior

None

Impact on communication

If an entry is changed when an access list is applied to an interface, packets received at the interface might be discarded temporarily until the entry is applied to the interface.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If *nnnn.nnnn.nnnn* `ffff.ffff.ffff` is entered as the source address and the destination address, `any` is displayed.
2. If the destination MAC address name or the address of the destination MAC address name is entered for the destination MAC address, the destination MAC address name is displayed.

   If *nnnn.nnnn.nnnn* `0000.0000.0000` is entered as the source address and the destination address in cases other than the above, `host` *nnnn.nnnn.nnnn* is displayed.

Related commands

```
mac access-group
mac access-list resequence
deny (mac access-list extended)
remark
```

remark

Sets supplementary information for an access list. Access lists are available for IPv4 address filtering, IPv4 packet filtering, IPv6 filtering, MAC filtering, and Advance. filtering

Syntax

To set or change information:

```
remark <remark>
```

To delete information:

```
no remark
```

Input mode

```
(config-ext-nacl)
(config-std-nacl)
(config-ipv6-acl)
(config-ext-macl)
(config-adv-acl)
```

Parameters

<remark>

Sets supplementary information according to input mode.

One line can be set for each access list. Entering new information overwrites the existing information.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify a character string with no more than 64 characters. Enclose it in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
advance access-list
ip access-list standard
ip access-list extended
ipv6 access-list
mac access-list extended
```

Chapter
3. QoS

Number of QoS flow lists and number of policer entries
Names and values that can be specified
advance qos-flow-group
advance qos-flow-list
advance qos-flow-list resequence
ip qos-flow-group
ip qos-flow-list
ip qos-flow-list resequence
ipv6 qos-flow-group
ipv6 qos-flow-list
ipv6 qos-flow-list resequence
mac qos-flow-group
mac qos-flow-list
mac qos-flow-list resequence
policer
qos (advance qos-flow-list)
qos (ip qos-flow-list)
qos (ipv6 qos-flow-list)
qos (mac qos-flow-list)
qos-queue-group
qos-queue-list
remark
traffic-shape rate

Number of QoS flow lists and number of policer entries

Number of policer entries

The number of policer entries is the number of policer entry names that are used as policer entry identifiers. A maximum of 128000 entries can be created for <*policer name*> of the relevant configuration for each of the receiving side and sending side. Specifications are counted separately for the receiving side and sending side.

Number of QoS flow lists

The number of QoS flow lists is the number of names that can be used as QoS flow list IDs. A maximum of 100608 lists can be created for <*qos flow list name*> of a relevant configuration.

Number of sequences

The number of sequences refers to the number of qos commands created.

A maximum of 256000 entries can be created for the QoS flow lists overall. The number of sequences here also includes the number of sequences of the access list.

Number of QoS flow lists that can be set for an interface

The number of QoS flow lists that can be set for an interface is the total number of QoS flow lists that can be set for an interface. A maximum of 100608 lists can be created.

If a QoS flow list is created and is not set for the interface, this QoS flow list is not counted in the number of QoS flow lists that can be set for the interface.

If a single QoS flow list is set for multiple interfaces, each list is counted as a separate list.

If multiple QoS flow lists are set for a single interface, each list is counted as a separate list. In this case, the receiving side and sending side are each counted as separate lists. For example, if a QoS flow list is set for both the receiving side and sending side of the same interface, two lists are counted regardless of whether the same QoS flow list name is specified.

Number of sequences that can be set for an interface

The number of sequences that can be set for an interface refers to the total number of sequences that can be set for an interface. A maximum of 256000 entries can be created. The number of sequences here also includes the number of sequences that can be set for the interfaces of access lists.

If a QoS flow list where a sequence has not been set is set for an interface, this QoS flow list is not counted in the number of sequences that can be set for the interface.

If a QoS flow list where a sequence has been set is set for an interface, it is counted as a separate entry for each QoS flow list that is set for the interface even if the QoS flow list name is the same.

Examples of calculating the number of QoS flow lists and number of sequences

The following table describes examples of calculating the number of QoS flow lists and the number of sequences.

Table 3-1: Examples of calculating the number of QoS flow lists and number of sequences

Sample code	Number of QoS flow lists to use	Number of QoS flow lists that can be set for an interface to be used	Number of sequences to be used	Number of sequences that can be set for an interface to be used

In this example, QoS flow list `AAA` is created and applied to inbound on Ethernet interface 2/1.
`interface gigabitethernet 2/1`
` ip qos-flow-group AAA in`
 	
`ip qos-flow-list AAA`
` 10 qos tcp any any action replace-dscp 3`
` 20 qos udp any any action discard-class 1`
	1 list	1 list	2 entries	2 entries

In this example, QoS flow list `AAA` is created and applied inbound on Ethernet interfaces 2/1 and 2/2.
`interface gigabitethernet 2/1`
` ip qos-flow-group AAA in`
 	
`interface gigabitethernet 2/2`
` ip qos-flow-group AAA in`
 	
`ip qos-flow-list AAA`
` 10 qos tcp any any action replace-dscp 3`
` 20 qos udp any any action discard-class 1`
	1 list	2 lists	2 entries	4 entries

In this example, QoS flow list `AAA` is created and applied to inbound and outbound on Ethernet interface 2/1.
`interface gigabitethernet 2/1`
` ip qos-flow-group AAA in`
` ip qos-flow-group AAA out`
 	
`ip qos-flow-list AAA`
` 10 qos tcp any any action replace-dscp 3`
` 20 qos udp any any action replace-dscp 3`
	1 list	2 lists	2 entries	4 entries

In this example, QoS flow list `AAA` is created and applied to inbound on Ethernet interface 2/1.
In this example, QoS flow list `BBB` is created and applied to inbound on Ethernet interface 2/2.
`interface gigabitethernet 2/1`
` ip qos-flow-group AAA in`
 	
`interface gigabitethernet 2/2`
` ip qos-flow-group BBB in`
 	
`ip qos-flow-list AAA`
` 10 qos tcp any any action replace-dscp 3`
` 20 qos udp any any action replace-dscp 3`
 	
`ip qos-flow-list BBB`
` 10 qos udp any any action replace-dscp 3`
` 20 qos tcp any any action discard-class 1`
	2 lists	2 lists	4 entries	4 entries

Sample code	Number of QoS flow lists to use	Number of QoS flow lists that can be set for an interface to be used	Number of sequences to be used	Number of sequences that can be set for an interface to be used

In this example, QoS flow list `AAA` is created and applied to inbound on Ethernet interface 2/1.
In this example, QoS flow list `BBB` is created and applied to outbound on Ethernet interface 2/1.
`interface gigabitethernet 2/1`
` ip qos-flow-group AAA in`
` ip qos-flow-group BBB out`
 	
`ip qos-flow-list AAA`
` 10 qos tcp any any action replace-dscp 3`
` 20 qos udp any any action replace-dscp 3`
 	
`ip qos-flow-list BBB`
` 10 qos udp any any action replace-dscp 3`
` 20 qos tcp any any action discard-class 1`
	2 lists	2 lists	4 entries	4 entries

In this example, QoS flow list `AAA` is created but not applied to any interface.
`ip qos-flow-list AAA`
` 10 qos tcp any any action replace-dscp 3`
	1 list	0 list	1 entry	0 entry

Names and values that can be specified

Protocol names (IPv4)

The following table lists the names that can be specified as IPv4 protocol names.

Table 3-2: Protocol names that can be specified (IPv4)

Protocol name	Applicable protocol number
ah	51
esp	50
gre	47
icmp	1
igmp	2
ip	All IP protocols
ipinip	4
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	41
udp	17
vrrp	112

Protocol names (IPv6)

The following table lists the names that can be specified as IPv6 protocol names.

Table 3-3: Protocol names that can be specified (IPv6)

Protocol name	Applicable protocol number
gre	47
icmp	58
ipv6	All IP protocols
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	4
udp	17

Protocol name	Applicable protocol number
vrrp	112

Port names (TCP)

The following table lists the port names that can be specified for TCP.

Table 3-4: Port names that can be specified for TCP

Port name	Applicable port name and number
bgp	Border Gateway Protocol version 4 (179)
chargen	Character generator (19)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
exec	Remote process execution (512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (20)
gopher	Gopher (70)
hostname	NIC Host Name Server (101)
http	HyperText Transfer Protocol (80)
https	HTTP over TLS/SSL (443)
ident	Ident Protocol (113)
imap3	Interactive Mail Access Protocol version 3 (220)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)
lpd	Printer service (515)
nntp	Network News Transfer Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
pop3s	POP3 over TLS/SSL (995)
raw	Printer PDL Data Stream (9100)
shell	Remote commands (514)
smtp	Simple Mail Transfer Protocol (25)

Port name	Applicable port name and number
smtps	SMTP over TLS/SSL (465)
ssh	Secure Shell Remote Login Protocol (22)
sunrpc	Sun Remote Procedure Call (111)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nicname (43)

Port names (UDP)

The following table lists the port names that can be specified for UDP.

Table 3-5: Port names that can be specified for UDP (IPv4)

Port name	Applicable port name and number
biff	Biff (512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)

Port name	Applicable port name and number
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

Table 3-6: Port names that can be specified for UDP (IPv6)

Port name	Applicable port name and number
biff	Biff (512)
dhcpv6-client	DHCPv6 client (546)
dhcpv6-server	DHCPv6 server (547)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
ripng	Routing Information Protocol next generation (521)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

tos names

The following table lists the tos names that can be specified.

Table 3-7: tos names that can be specified

tos name	tos value
max-reliability	2
max-throughput	4
min-delay	8
min-monetary-cost	1
normal	0

precedence names

The following table lists the precedence names that can be specified.

Table 3-8: precedence names that can be specified

precedence name	precedence value
critical	5
flash	3
flash-override	4
immediate	2
internet	6
network	7
priority	1
routine	0

DSCP names

The following table lists the DSCP names that can be specified.

Table 3-9: DSCP names that can be specified

DSCP name	DSCP value
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38

DSCP name	DSCP value
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
default	0
ef	46

Ethernet type names

The following table lists the Ethernet type names that can be specified.

Table 3-10: Ethernet type names that can be specified

Ethernet type name	Ethernet value	Remarks
appletalk	0x809b	
arp	0x0806	
axp	0x88f3	Alaxala Protocol
eapol	0x888e	
gsrp	--#	Displays GSRP control packets.
ipv4	0x0800	
ipv6	0x86dd	
ipx	0x8137	
xns	0x0600	

#: The value is not made public.

Destination MAC address names

The following table lists the destination MAC address names that can be specified.

Table 3-11: Destination MAC address names that can be specified

Destination address specification	Destination address	Destination address mask
bpdu	0180.C200.0000	0000.0000.0000
broadcast	FFFF.FFFF.FFFF	0000.0000.0000
cdp	0100.0CCC.CCCC	0000.0000.0000
lldp	0180.C200.000E	0000.0000.0000
multicast#	0100.0000.0000	FEFF.FFFF.FFFF
oadp	0100.4C79.FD1B	0000.0000.0000

Destination address specification	Destination address	Destination address mask
pvst-plus-bpdu	0100.0CCC.CCCD	0000.0000.0000
slow-protocol	0180.C200.0002	0000.0000.0000

#: Includes broadcast packets.

Message names (ICMP)

The following table lists the message names that can be specified for ICMP.

Table 3-12: Message names that can be specified for ICMP (IPv4)

Message name	Message	Type	Code
administratively-prohibited	Administratively prohibited	3	13
alternate-address	Alternate address	6	Not specified
conversion-error	Datagram conversion	31	Not specified
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	Not specified
echo-reply	Echo reply	0	Not specified
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1
information-reply	Information replies	16	Not specified
information-request	Information requests	15	Not specified
mask-reply	Mask replies	18	Not specified
mask-request	Mask requests	17	Not specified
mobile-redirect	Mobile host redirect	32	Not specified
net-redirect	Network redirect	5	0
net-tos-redirect	Network redirect for TOS	5	2
net-tos-unreachable	Network unreachable for TOS	3	11
net-unreachable	Network unreachable	3	0
network-unknown	Network unknown	3	6
no-room-for-option	Parameter required but no room	12	2

Message name	Message	Type	Code
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4
parameter-problem	All parameter problems	12	Not specified
port-unreachable	Port unreachable	3	3
precedence-unreachable	Precedence cutoff	3	15
protocol-unreachable	Protocol unreachable	3	2
reassembly-timeout	Reassembly timeout	11	1
redirect	All redirects	5	Not specified
router-advertisement	Router discovery advertisements	9	Not specified
router-solicitation	Router discovery solicitations	10	Not specified
source-quench	Source quenches	4	Not specified
source-route-failed	Source route failed	3	5
time-exceeded	All time exceeded	11	Not specified
timestamp-reply	Timestamp replies	14	Not specified
timestamp-request	Timestamp requests	13	Not specified
traceroute	Traceroute	30	Not specified
ttl-exceeded	TTL exceeded	11	0
unreachable	All unreachable	3	Not specified

Table 3-13: Message names that can be specified for ICMP (IPv6)

Message name	Message	Type	Code
beyond-scope	Destination beyond scope	1	2
destination-unreachable	Destination address is unreachable	1	3
echo-reply	Echo reply	129	Not specified
echo-request	Echo request (ping)	128	Not specified
header	Parameter header problems	4	0
hop-limit	Hop limit exceeded in transit	3	0
mld-query	Multicast Listener Discovery Query	130	Not specified
mld-reduction	Multicast Listener Discovery Reduction	132	Not specified
mld-report	Multicast Listener Discovery Report	131	Not specified
nd-na	Neighbor discovery neighbor advertisements	136	Not specified
nd-ns	Neighbor discovery neighbor solicitations	135	Not specified
next-header	Parameter next header problems	4	1
no-admin	Administration prohibited destination	1	1
no-route	No route to destination	1	0

Message name	Message	Type	Code
packet-too-big	Packet too big	2	Not specified
parameter-option	Parameter option problems	4	2
parameter-problem	All parameter problems	4	Not specified
port-unreachable	Port unreachable	1	4
reassembly-timeout	Reassembly timeout	3	1
renum-command	Router renumbering command	138	0
renum-result	Router renumbering result	138	1
renum-seq-number	Router renumbering sequence number reset	138	255
router-advertisement	Neighbor discovery router advertisements	134	Not specified
router-renumbering	All router renumbering	138	Not specified
router-solicitation	Neighbor discovery router solicitations	133	Not specified
time-exceeded	All time exceeded	3	Not specified
unreachable	All unreachable	1	Not specified

advance qos-flow-group

Applies an Advance QoS flow list to an interface, and enables the QoS functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

Syntax

To set information:

```
advance qos-flow-group <qos flow list name> {in | out}
```

To delete information:

```
no advance qos-flow-group <qos flow list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<qos flow list name>

Specifies the Advance QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This can be set when the flow detection mode is `condition-oriented`.
2. One can be set for each inbound and outbound side of the same interface. If it is already set, delete before specifying the setting.
3. If a non-existent Advance QoS flow list name is set, no operation is performed. The Advance QoS flow list name is registered.
4. This can be set if an IPv4 address is set for the target interface when `mac-ip` is specified for the flow detection condition type, and there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
5. This can be set if a single IPv6 global address only is set for the target interface when `mac-ipv6` is specified for the flow detection condition type, and there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
6. If the specified content of the receiving side and sending side of the policer entry and this command are identical, the Advance QoS flow list specified by the policer entry can be applied to the interface.

Related commands

```
advance qos-flow-list
flow detection mode
```

advance qos-flow-list

Sets an Advance QoS flow list to be used to set QoS flow detection and action specifications. After this command is executed, the mode changes to `config-adv-qos` mode.

Syntax

To set information:

```
advance qos-flow-list <qos flow list name>
```

To delete information:

```
no advance qos-flow-list <qos flow list name>
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the Advance QoS flow list name.

QoS flow list names that are already being used in the IPv4 QoS flow list, IPv6 QoS flow list, and MAC QoS flow list cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
advance qos-flow-group
advance qos-flow-list resequence
qos (advance qos-flow-list)
remark
```

advance qos-flow-list resequence

Resets the sequence numbers of the application sequence in the Advance QoS flow list.

Syntax

To set or change information:

```
advance qos-flow-list resequence <qos flow list name> [<starting sequence>
[<increment sequence>]]
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the Advance QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
        advance qos-flow-list
```

ip qos-flow-group

Applies an IPv4 QoS flow list to an interface, and enables the QoS functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

Syntax

To set information:

```
ip qos-flow-group <qos flow list name> {in | out}
```

To delete information:

```
no ip qos-flow-group <qos flow list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<qos flow list name>

Specifies the IPv4 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One can be set for each inbound and outbound side of the same interface. If it is already set, delete before specifying the setting.
2. If a non-existent IPv4 QoS flow list name is set, no operation is performed. The IPv4 QoS flow list name is registered.
3. This can be set if an IPv4 address is set for the target interface when there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
4. If the specified content of the receiving side and sending side of the policer entry and this command are identical, the IPv4 QoS flow list specified by the policer entry can be applied to the interface.

Related commands

```
ip qos-flow-list
```

ip qos-flow-list

Sets an IPv4 QoS flow list to be used to set QoS flow detection and action specifications. After this command is executed, the mode changes to `config-ip-qos` mode.

Syntax

To set information:

```
ip qos-flow-list <qos flow list name>
```

To delete information:

```
no ip qos-flow-list <qos flow list name>
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the IPv4 QoS flow list name.

QoS flow list names that are already being used in the IPv6 QoS flow list, MAC QoS flow list, and Advance QoS flow list cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ip qos-flow-group
ip qos-flow-list resequence
qos (ip qos-flow-list)
remark
```

ip qos-flow-list resequence

Resets the sequence numbers of the application sequence in the IPv4 QoS flow list.

Syntax

To set or change information:

```
ip qos-flow-list resequence <qos flow list name> [<starting sequence>
[<increment sequence>] ]
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the IPv4 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ip qos-flow-list
```

ipv6 qos-flow-group

Applies an IPv6 QoS flow list to an interface, and enables the QoS functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

Syntax

To set information:

```
ipv6 qos-flow-group <qos flow list name> {in | out}
```

To delete information:

```
no ipv6 qos-flow-group <qos flow list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<qos flow list name>

Specifies the IPv6 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One can be set for each inbound and outbound side of the same interface. If it is already set, delete before specifying the setting.
2. If a non-existent IPv6 QoS flow list name is set, no operation is performed. The IPv6 QoS flow list name is registered.
3. This can be set if a single IPv6 global address only is set for the target interface when there is an `own-address` or `own-prefix` parameter in the flow detection conditions.
4. This can be set if `any` or *<length>* of 64 or less is specified for the source address of the flow detection conditions parameter.
5. If the specified content of the receiving side and sending side of the policer entry and this command are identical, the IPv6 QoS flow list specified by the policer entry can be applied to the interface.

Related commands

```
ipv6 qos-flow-list
```

ipv6 qos-flow-list

Sets an IPv6 QoS flow list to be used to set QoS flow detection and action specifications. After this command is executed, the mode changes to `config-ipv6-qos` mode.

Syntax

To set information:

```
    ipv6 qos-flow-list <qos flow list name>
```

To delete information:

```
    no ipv6 qos-flow-list <qos flow list name>
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the IPv6 QoS flow list name.

QoS flow list names that are already being used in the IPv4 QoS flow list, MAC QoS flow list, and Advance QoS flow list cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ipv6 qos-flow-group
ipv6 qos-flow-list resequence
qos (ipv6 qos-flow-list)
remark
```

ipv6 qos-flow-list resequence

Resets the sequence numbers of the application sequence in the IPv6 QoS flow list.

Syntax

To set or change information:

```
ipv6 qos-flow-list resequence <qos flow list name> [<starting sequence>
[<increment sequence>] ]
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the IPv6 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.
2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.
2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ipv6 qos-flow-list
```

mac qos-flow-group

Applies a MAC QoS flow list to an interface, and enables the QoS functionality. The interfaces that can be applied are shown below:

- Ethernet interface
- Ethernet subinterface
- Port channel subinterface

Syntax

To set information:

```
mac qos-flow-group <qos flow list name> {in | out}
```

To delete information:

```
no mac qos-flow-group <qos flow list name> {in | out}
```

Input mode

`(config-if)`

Ethernet interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

<qos flow list name>

Specifies the MAC QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One can be set for each inbound and outbound side of the same interface. If it is already set, delete before specifying the setting.
2. If a non-existent MAC QoS flow list name is set, no operation is performed. The MAC QoS flow list name is registered.
3. If the specified content of the receiving side and sending side of the policer entry and this command are identical, the MAC QoS flow list specified by the policer entry can be applied to the interface.

Related commands

```
mac qos-flow-list
```

mac qos-flow-list

Sets an MAC QoS flow list to be used to set QoS flow detection and action specifications. After this command is executed, the mode changes to `config-mac-qos` mode.

Syntax

To set information:

```
mac qos-flow-list <qos flow list name>
```

To delete information:

```
no mac qos-flow-list <qos flow list name>
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the MAC QoS flow list name.

QoS flow list names that are already being used in the IPv4 QoS flow list, IPv6 QoS flow list, and Advance QoS flow list cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
mac qos-flow-group
mac qos-flow-list resequence
qos (mac qos-flow-list)
remark
```

mac qos-flow-list resequence

Resets the sequence numbers of the application sequence in the MAC QoS flow list.

Syntax

To set or change information:

```
mac qos-flow-list resequence <qos flow list name> [<starting sequence>
[<increment sequence>]]
```

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the MAC QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS flow list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
mac qos-flow-list
```

policer

Sets policer entries.

Syntax

To set or change information:

```
policer <policer name> {in | out} <bandwidth policy> [replace-user-priority
<priority>] [replace-dscp <dscp>] [discard-class <class>]
```

To delete information:

```
no policer <policer name>
```

- *<bandwidth policy>*:

When maximum bandwidth monitoring is specified:

```
max-rate {<kbit/s>k | <Mbit/s>M | <Gbit/s>G} [max-burst {<byte> | <kbyte>k |
<Mbyte>M | <Gbyte>G}]
```

When minimum bandwidth monitoring is specified:

```
min-rate {<kbit/s>k | <Mbit/s>M | <Gbit/s>G} [min-burst {<byte> | <kbyte>k |
<Mbyte>M | <Gbyte>G}] [penalty-user-priority <priority>] [penalty-dscp
<dscp>] [penalty-discard-class <class>]
```

When maximum bandwidth monitoring and minimum bandwidth monitoring are specified:

```
[max-rate {<kbit/s>k | <Mbit/s>M | <Gbit/s>G} [max-burst {<byte> | <kbyte>k
| <Mbyte>M | <Gbyte>G}]] [min-rate {<kbit/s>k | <Mbit/s>M | <Gbit/s>G}
[min-burst {<byte> | <kbyte>k | <Mbyte>M | <Gbyte>G}] [penalty-user-priority
<priority>] [penalty-dscp <dscp>] [penalty-discard-class <class>]]
```

Input mode

`(config)`

Parameters

<policer name>

Specifies the policer entry name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a policer entry name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{in | out}

Specifies inbound or outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<bandwidth policy> parameter

max-rate {<*kbit/s*>k | <*Mbit/s*>M | <*Gbit/s*>G}

Specifies the monitoring bandwidth value for maximum bandwidth monitoring. Discards non-compliant packets that have exceeded the specified bandwidth value. Specify a value that is equal to `min-rate` or larger.

Always specify either this parameter or `min-rate`.

1. Default value when this parameter is omitted:

   None (Maximum bandwidth monitoring is not performed.)

2. Range of values:

   <*kbit/s*>: 5 to 100000000 (in decimal)

   <*Mbit/s*>: 1 to 100000 (in decimal)

   <*Gbit/s*>: 1 to 100 (in decimal)

   1 kbit/s, 1 Mbit/s, and 1 Gbit/s are handled as 1000 bit/s, 1000 kbit/s, and 1000 Mbit/s, respectively.

max-burst {<*byte*> | <*kbyte*>k | <*Mbyte*>M | <*Gbyte*>G}

Specifies the burst size in maximum bandwidth monitoring. Specify a value that is equal to `min-burst` or larger.

1. Default value when this parameter is omitted:

   <*byte*>: 65536

2. Range of values:

   <*byte*>: 3076 to 4294967296 (in decimal)

   <*kbyte*>: 4 to 4194304 (in decimal)

   <*Mbyte*>: 1 to 4096 (in decimal)

   <*Gbyte*>: 1 to 4 (in decimal)

   1 kbyte, 1 Mbyte, and 1 Gbyte are handled as 1024 byte, 1024 kbyte, and 1024 Mbyte, respectively.

min-rate {<*kbit/s*>k | <*Mbit/s*>M | <*Gbit/s*>G}

Specifies the monitoring bandwidth value for minimum bandwidth monitoring. Penalizes non-compliant packets that have exceeded the specified monitoring bandwidth value. Specify a value that is equal to `max-rate` or fewer.

Always specify either this parameter or `max-rate`.

1. Default value when this parameter is omitted:

   None (Minimum bandwidth monitoring is not performed.)

2. Range of values:

   <*kbit/s*>: 5 to 100000000 (in decimal)

   <*Mbit/s*>: 1 to 100000 (in decimal)

   <*Gbit/s*>: 1 to 100 (in decimal)

   1 kbit/s, 1 Mbit/s, and 1 Gbit/s are handled as 1000 bit/s, 1000 kbit/s, and 1000 Mbit/s, respectively.

min-burst {<*byte*> | <*kbyte*>k | <*Mbyte*>M | <*Gbyte*>G }

Specifies the burst size in minimum bandwidth monitoring. Specify a value that is equal to `max-burst` or fewer.

1. Default value when this parameter is omitted:

<*byte*>: 65536

2. Range of values:

   <*byte*>: 3076 to 4294967296 (in decimal)

   <*kbyte*>: 4 to 4194304 (in decimal)

   <*Mbyte*>: 1 to 4096 (in decimal)

   <*Gbyte*>: 1 to 4 (in decimal)

   1 kbyte, 1 Mbyte, and 1 Gbyte are handled as 1024 byte, 1024 kbyte, and 1024 Mbyte, respectively.

penalty-user-priority <*priority*>

Specifies the value for rewriting the user priority when non-compliance occurs in minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

   None (User priority is not overwritten when non-compliance occurs in minimum bandwidth monitoring.)

2. Range of values:

   Specify 0 to 7 in decimal.

penalty-dscp <*dscp*>

Specifies the value for rewriting DSCP when non-compliance occurs in minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

   None (DSCP value is not overwritten when non-compliance occurs in minimum bandwidth monitoring.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

penalty-discard-class <*class*>

Specifies the discard class when non-compliance occurs in minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

   None (Discard class is not specified when non-compliance occurs in minimum bandwidth monitoring.)

2. Range of values:

   Specify 1 to 4 in decimal.

replace-user-priority <*priority*>

Specifies the value for rewriting the user priority.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

replace-dscp <*dscp*>

Specifies the value for rewriting DSCP.

1. Default value when this parameter is omitted:

   None. (The DSCP value is not replaced.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

discard-class <*class*>

Specifies the discard class.

1. Default value when this parameter is omitted:

   None (The discard class is not changed.)

2. Range of values:

   Specify 1 to 4 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This cannot be deleted if it was specified as an operation of the QoS flow list. Before executing, delete the specified operation for the relevant policer entry from the QoS flow list.
2. `max-rate` and `min-rate` can be entered in any order. Also, the `show running-config` operation command is displayed in the input order.

Related commands

```
qos (advance qos-flow-list)
qos (ip qos-flow-list)
qos (ipv6 qos-flow-list)
qos (mac qos-flow-list)
```

qos (advance qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv6 QoS flow list.

Syntax

To set or change information:

```
[<sequence>] qos mac <target flow> [<action specification>]
[<sequence>] qos mac-ip <target flow> [<action specification>]
[<sequence>] qos mac-ipv6 <target flow> [<action specification>]
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

For `mac` *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions.

```
mac {<source mac> <source mac mask> | host <source mac> | any} {<destination
mac> <destination mac mask> | host <destination mac> | any | <destination mac
name>} [<ethernet type>] [{untagged | [user-priority <priority>] [tag-vlan
<vlan id>]}]
```

For `mac-ip` *<target flow>*:

This flow detection condition is used to perform flow detection based on MAC header conditions, VLAN Tag header conditions, IPv4 header conditions, or Layer 4 header conditions.

If the `+fo` parameter is set for the flow detection conditions, the MAC header conditions, VLAN tag header conditions, and IPv4 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, ICMP, and IGMP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ip | <protocol>} {{<source ipv4> |
own-address} <source ipv4 wildcard> | host {<source ipv4> | own-address}
| any | own-prefix | range-address <source ipv4 start> <source ipv4 end>}
{{<destination ipv4> | own-address} <destination ipv4 wildcard> | host
{<destination ipv4> | own-address} | any | own-prefix | range-address
<destination ipv4 start> <destination ipv4 end>} [{[tos <tos>]
[precedence <precedence>] | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
mac-ip {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} tcp {{<source ipv4> | own-address} <source ipv4
wildcard> | host {<source ipv4> | own-address} | any | own-prefix |
range-address <source ipv4 start> <source ipv4 end>} [{{eq | neq} <source
port> | range <source port start> <source port end>}] {{<destination
ipv4> | own-address} <destination ipv4 wildcard> | host {<destination
ipv4> | own-address} | any | own-prefix | range-address <destination ipv4
start> <destination ipv4 end>} [{{eq | neq} <destination port> | range
<destination port start> <destination port end>}] [{[established] |
[{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}] [{+rst | -rst}] [{+syn |
-syn}] [{+urg | -urg}]}] [{[tos <tos>] [precedence <precedence>] | dscp
<dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged
```

| [user-priority <*priority*>] [tag-vlan <*vlan id*>]}]

When the +fo parameter is not specified and the upper layer protocol is UDP:

mac-ip {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | <*destination mac name*>} udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>} [{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}] {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [length {upper | lower} <*length*>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <*priority*>] [tag-vlan <*vlan id*>]}]

When the +fo parameter is not specified and the upper layer protocol is ICMP:

mac-ip {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | <*destination mac name*>} icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [length {upper | lower} <*length*>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <*priority*>] [tag-vlan <*vlan id*>]}]

When the +fo parameter is not specified and the upper layer protocol is IGMP:

mac-ip {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | <*destination mac name*>} igmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [<*igmp type*>] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [length {upper | lower} <*length*>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <*priority*>] [tag-vlan <*vlan id*>]}]

When the +fo parameter is specified:

mac-ip {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | <*destination mac name*>} {ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [length {upper | lower} <*length*>] [{+mf | -mf}] [+fo] [{untagged | [user-priority <*priority*>] [tag-vlan <*vlan id*>]}]

For mac-ipv6 <*target flow*>:

This flow detection condition is used to perform flow detection based on MAC header conditions, VLAN Tag header conditions, IPv6 header conditions, or Layer 4 header conditions.

If the +fo parameter is set for the flow detection conditions, the MAC header conditions, VLAN tag header conditions, and IPv6 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

When the +fo parameter is not specified and the upper layer protocol is a type other than TCP, UDP, and ICMP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ipv6 | <protocol>} {<source ipv6>/<length>|
host {<source ipv6> | own-address} | any | own-address <own address
length> | own-prefix | range-address <source ipv6 start> <source ipv6
end>} {<destination ipv6>/<length>| host {<destination ipv6> |
own-address} | any | own-address <own address length> | own-prefix |
range-address <destination ipv6 start> <destination ipv6 end>}
[{traffic-class <traffic class> | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is TCP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} tcp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any | own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq}
<source port> | range <source port start> <source port end>}]
{<destination ipv6>/<length>| host {<destination ipv6> | own-address} |
any | own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port
end>}] [{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}]
[{+rst | -rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{traffic-class
<traffic class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf
| -mf}] [-fo] [{untagged | [user-priority <priority>] [tag-vlan <vlan
id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is UDP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} udp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any | own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} [{{eq | neq}
<source port> | range <source port start> <source port end>}]
{<destination ipv6>/<length>| host {<destination ipv6> | own-address} |
any | own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port
end>}] [{traffic-class <traffic class> | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | [user-priority
<priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is not specified and the upper layer protocol is ICMP:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} icmp {<source ipv6>/<length>| host {<source
ipv6> | own-address} | any | own-address <own address length> | own-prefix
| range-address <source ipv6 start> <source ipv6 end>} {<destination
ipv6>/<length>| host {<destination ipv6> | own-address} | any |
own-address <own address length> | own-prefix | range-address
<destination ipv6 start> <destination ipv6 end>} [{<icmp type> [<icmp
code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged |
[user-priority <priority>] [tag-vlan <vlan id>]}]
```

When the +fo parameter is specified:

```
mac-ipv6 {<source mac> <source mac mask> | host <source mac> | any}
{<destination mac> <destination mac mask> | host <destination mac> | any
| <destination mac name>} {ipv6 | <protocol> | icmp | tcp | udp} {<source
ipv6>/<length>| host {<source ipv6> | own-address} | any | own-address
<own address length> | own-prefix | range-address <source ipv6 start>
<source ipv6 end>} {<destination ipv6>/<length>| host {<destination ipv6>
| own-address} | any | own-address <own address length> | own-prefix |
range-address <destination ipv6 start> <destination ipv6 end>}
[{traffic-class <traffic class> | dscp <dscp>}] [length {upper | lower}
<length>] [{+mf | -mf}] [+fo] [{untagged | [user-priority <priority>]
[tag-vlan <vlan id>]}]
```

- *<action specification>*:

For `mac` *<target flow>* `[`*<action specification>*`]`:

When no policer entry is included:

```
action [replace-user-priority <priority>] [replace-dscp <dscp>]
[priority-class <class>] [discard-class <class>]
```

When a policer entry is included:

```
action [policer <policer name>] [priority-class <class>]
```

For `mac-ip` *<target flow>* `[`*<action specification>*`]` or `mac-ipv6` *<target flow>* `[`*<action specification>*`]`:

When no policer entry is included:

```
action [replace-user-priority <priority>] [replace-dscp <dscp>]
[{[priority-class <class>] [discard-class <class>] | dscp-map}]
```

When a policer entry is included:

```
action [policer <policer name>] [{priority-class <class> | dscp-map}]
```

Input mode

`(config-adv-qos)`

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the QoS flow list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{*<source mac>* *<source mac mask>* | host *<source mac>* | any}

Specifies the source MAC address.

If `host` *<source mac>* is specified, the flow detection condition is an exact match of *<source mac>*.

To specify all source MAC addresses, specify `any`. If `any` is specified, the source MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source MAC address for *<source mac>*.

For <*source mac mask*>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | <*destination mac name*>}

Specifies the destination MAC address.

If `host` <*destination mac*> is specified, the flow detection condition is an exact match of <*destination mac*>.

To specify all destination MAC addresses, specify `any`. If `any` is specified, the destination MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination MAC address for <*destination mac*>.

   For <*destination mac mask*>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   Specify the destination MAC address for <*destination mac name*>. For details about the destination MAC address names that can be specified, see *Table 3-11: Destination MAC address names that can be specified*.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<*ethernet type*>

Specifies the Ethernet type value.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name.

   For details about the Ethernet type names that can be specified, see *Table 3-10: Ethernet type names that can be specified*.

untagged

Specifies detection of untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

tag-vlan <*vlan id*>

Specifies the VLAN ID of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 4095 in decimal.

{ip | <*protocol*> | icmp | igmp | tcp | udp}

You can select this parameter when `mac-ip` is specified as the flow detection condition.

Specifies the upper-layer protocol condition for IPv4 packets. Note that if all protocols are applicable, specify `ip`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set 0 to 255 (in decimal) or a protocol name.

   For details about the protocol names that can be specified, see *Table 3-2: Protocol names that can be specified (IPv4)*.

{ipv6 | <*protocol*> | icmp | tcp | udp}

You can select this parameter when `mac-ipv6` is specified as the flow detection condition.

Specifies the upper-layer protocol condition for IPv6 packets. Note that if all protocols are applicable, specify `ipv6`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 42, 45 to 49, 52 to 59, 61 to 255 (in decimal), or a protocol name.

   For details about the protocol names that can be specified, see *Table 3-3: Protocol names that can be specified (IPv6)*.

{{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own-prefix | range-address <*source ipv4 start*> <*source ipv4 end*>}

Specifies the source IPv4 address.

If `host` <*source ipv4*> is specified, the flow detection condition is an exact match of <*source ipv4*>.

To specify all source IPv4 addresses, specify `any`. If `any` is specified, the source IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the source IPv4 address.

If `own-prefix` is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*source* *ipv4 start*> to <*source ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv4 address for <*source ipv4*>.

   For <*source ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*source ipv4 end*> is larger than <*source ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*source ipv6 start*> <*source ipv6 end*>}

Specifies the source IPv6 address.

If `host` <*source ipv6*> is specified, the flow detection condition is an exact match of <*source ipv6*>.

To specify all source IPv6 addresses, specify `any`. If `any` is specified, the source IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the source IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the source IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*source ipv6 start*> to <*source ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv6 address for <*source ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

   Specify IPv6 addresses so that <*source ipv6 end*> is larger than <*source ipv6 start*>.

   <*source ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <*length*>: 0 to 128

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be specified, see *Table 3-4: Port names that can be specified for TCP*, *Table 3-5: Port names that can be specified for UDP (IPv4)*, or *Table 3-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own-prefix | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

If `host` <*destination ipv4*> is specified, the flow detection condition is an exact match of <*destination ipv4*>.

To specify all destination IPv4 addresses, specify `any`. If `any` is specified, the destination IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the target IPv4 address.

If `own-prefix` is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv4 start*> to <*destination ipv4 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv4 address for <*destination ipv4*>.

   For <*destination ipv4 wildcard*>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that <*destination ipv4 end*> is larger than <*destination ipv4 start*>.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

If `host` <*destination ipv6*> is specified, the flow detection condition is an exact match of <*destination ipv6*>.

To specify all destination IPv6 addresses, specify `any`. If `any` is specified, the destination IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the target IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the target IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv6 start*> to <*destination ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv6 address for <*destination ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

   Specify IPv6 addresses so that <*destination ipv6 end*> is larger than <*destination ipv6 start*>.

   <*destination ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <*length*>: 0 to 128

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*destination port*>.

If `neq` is specified, the flow detection condition is other than <*destination port*>.

If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be specified, see *Table 3-4: Port names that can be specified for TCP*, *Table 3-5: Port names that can be specified for UDP (IPv4)*, or *Table 3-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

tos <*tos*>

Specifies 4 bits (bits 3 to 6) in the ToS field as the tos value.

The TOS value is compared with 4 bits (bits 3 to 6) in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 3-7: tos names that can be specified*.

precedence <*precedence*>

Specifies the precedence value, which is the first 3 bits in the ToS field.

Its value is compared with the first 3 bits in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 3-8: precedence names that can be specified*.

traffic-class <*traffic class*>

Specifies the traffic class field value.

Its value is compared with the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

dscp <*dscp*>

- When the flow detection condition type is `mac-ip`:

  Specifies the DSCP value, which is the first 6 bits in the ToS field.

  Its value is compared with the first 6 bits in the ToS field of the received packet.

- When the flow detection condition type is `mac-ipv6`:

  Specifies the DSCP value, which is the first 6 bits in the traffic class field.

  Its value is compared with the first 6 bits in the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<*icmp type*>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<*icmp code*>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<*icmp message*>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be set, see *Table 3-12: Message names that can be specified for ICMP (IPv4)* or *Table 3-13: Message names that can be specified for ICMP (IPv6)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<igmp type>

Specifies the IGMP type.

This parameter option is available only if the protocol is IGMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

length {upper | lower} *<length>*

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of *<length>* or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of *<length>* or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

- When the flow detection condition type is `mac-ip`:

  Specifies the MF flag value, which is the lower 1 bit in the Flags field.

  `+mf` indicates a packet where an MF flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an MF flag of 0 is set for the flow detection conditions.

- When the flow detection condition type is `mac-ipv6`:

  Specifies the M flag value of the fragment header.

  `+mf` indicates a packet where an M flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an M flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<*action specification*> parameter

action

Specifies the operation of the packet where a flow was detected. Specify the start of the entire <*action specification*> parameter.

1. Default value when this parameter is omitted:

   None (No operation is specified.)

2. Range of values:

   None

priority-class <*class*>

Specifies the priority class.

1. Default value when this parameter is omitted:

   None (The priority class is not changed.)

2. Range of values:

   Specify 1 to 8 in decimal.

discard-class <*class*>

Specifies the discard class.

The discard class of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

   None (The discard class is not changed.)

2. Range of values:

   Specify 1 to 4 in decimal.

replace-dscp <*dscp*>

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the <*dscp*> value.

1. Default value when this parameter is omitted:

   None. (The DSCP value is not replaced.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

replace-user-priority <*priority*>

Specifies the value for rewriting the user priority.

Replace the user priority of the received packet with <*priority*>.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

dscp-map

Enables DSCP mapping which determines the priority class and discard class based on the DSCP value.

For details on the priority class and discard class corresponding to the DSCP values, see the *6. Priority Change* in the manual *Configuration Guide Vol. 2 For Version 12.1*.

1. Default value when this parameter is omitted:

   None (DSCP mapping is not used.)

2. Range of values:

   None

policer <*policer name*>

Specifies the policer entry name.

1. Default value when this parameter is omitted:

   None (Policer function is not used.)

2. Range of values:

   Specifies the policer entry name that was set by the policer command.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If *nnnn.nnnn.nnnn* `ffff.ffff.ffff` is entered as the source MAC address and the destination MAC address, `any` is displayed.
2. If the destination MAC address name or the address of the destination MAC address name is entered for the destination MAC address, the destination MAC address name is displayed.

   If *nnnn.nnnn.nnnn* `0000.0000.0000` is entered as the source MAC address and the destination MAC address in cases other than the above, `host` *nnnn.nnnn.nnnn* is displayed.
3. If `255.255.255.255` is entered for the source IPv4 address wildcard mask and the destination IPv4 address wildcard mask, `any` is displayed.
4. If `0.0.0.0` is entered for the source IPv4 address wildcard mask and the destination IPv4 address wildcard mask, `host` *nnn.nnn.nnn.nnn*, `host own-address` is displayed.
5. If 0 is entered for the <*length*> or <*own address length*> of the source IPv6 address and destination IPv6 address, `any` is displayed.
6. If 128 is entered for the <*length*> or <*own address length*> of the source IPv6 address and destination IPv6 address, `host` *nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn*, `host own-address` is displayed.

Related commands

```
advance qos-flow-list
advance qos-flow-group
advance qos-flow-list resequence
remark
policer
```

qos (ip qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv4 QoS flow list.

If the `+fo` parameter is set for the flow detection conditions, the VLAN tag header conditions and IPv4 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

Syntax

To set or change information:

```
[<sequence>] qos <target flow> [<action specification>]
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, ICMP, and IGMP:

```
{ip | <protocol>} {{<source ipv4> | own-address} <source ipv4 wildcard> |
host {<source ipv4> | own-address} | any | own-prefix | range-address <source
ipv4 start> <source ipv4 end>} {{<destination ipv4> | own-address}
<destination ipv4 wildcard> | host {<destination ipv4> | own-address} | any
| own-prefix | range-address <destination ipv4 start> <destination ipv4 end>}
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
tcp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} [{{eq | neq} <source port> | range <source port start>
<source port end>}] {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port
end>}][{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}] [{+rst
| -rst}] [{+syn|-syn}] [{+urg | -urg}]}] [{[tos <tos>] [precedence
<precedence>] | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}]
[-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is UDP:

```
udp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} [{{eq | neq} <source port> | range <source port start>
<source port end>}] {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{{eq | neq}
<destination port> | range <destination port start> <destination port end>}]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is ICMP:

```
icmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [{<icmp type>
[<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] |
dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged
| user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is IGMP:

```
igmp {{<source ipv4> | own-address} <source ipv4 wildcard> | host {<source
ipv4> | own-address} | any | own-prefix | range-address <source ipv4 start>
<source ipv4 end>} {{<destination ipv4> | own-address} <destination ipv4
wildcard> | host {<destination ipv4> | own-address} | any | own-prefix |
range-address <destination ipv4 start> <destination ipv4 end>} [<igmp type>]
[{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is specified:

```
{ip | <protocol> | icmp | igmp | tcp | udp} {{<source ipv4> | own-address}
<source ipv4 wildcard> | host {<source ipv4> | own-address} | any | own-prefix
| range-address <source ipv4 start> <source ipv4 end>} {{<destination ipv4>
| own-address} <destination ipv4 wildcard> | host {<destination ipv4> |
own-address} | any | own-prefix | range-address <destination ipv4 start>
<destination ipv4 end>} [{[tos <tos>] [precedence <precedence>] | dscp
<dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
user-priority <priority>}]
```

■ <*action specification*>:

When no policer entry is included:

```
action [replace-user-priority <priority>] [replace-dscp <dscp>]
[{[priority-class <class>] [discard-class <class>] | dscp-map}]
```

When a policer entry is included:

```
action [policer <policer name>] [{priority-class <class> | dscp-map}]
```

Input mode

```
(config-ip-qos)
```

Parameters

<*sequence*>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the QoS flow list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<*target flow*> parameter

{ip | <*protocol*> | icmp | igmp | tcp | udp}

Specifies the upper-layer protocol condition for IPv4 packets. Note that if all protocols are applicable, specify `ip`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set 0 to 255 (in decimal) or a protocol name.

   For details about the protocol names that can be specified, see *Table 3-2: Protocol names that can be specified (IPv4)*.

{{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> |

own-address} | any | own-prefix | range-address *<source ipv4 start> <source ipv4 end>*}

Specifies the source IPv4 address.

If `host` *<source ipv4>* is specified, the flow detection condition is an exact match of *<source ipv4>*.

To specify all source IPv4 addresses, specify `any`. If `any` is specified, the source IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the source IPv4 address.

If `own-prefix` is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from *<source ipv4 start>* to *<source ipv4 end>*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv4 address for *<source ipv4>*.

   For *<source ipv4 wildcard>*, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that *<source ipv4 end>* is larger than *<source ipv4 start>*.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{{eq | neq} *<source port>* | range *<source port start> <source port end>*}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of *<source port>*.

If `neq` is specified, the flow detection condition is other than *<source port>*.

If `range` is specified, the flow detection condition is in the range from *<source port start>* to *<source port end>*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 3-4: Port names that can be specified for TCP* or *Table 3-5: Port names that can be specified for UDP (IPv4)*.

   Specify port numbers so that *<source port end>* is larger than *<source port start>*.

{{*<destination ipv4>* | own-address} *<destination ipv4 wildcard>* | host {*<destination ipv4>* | own-address} | any | own-prefix | range-address *<destination ipv4 start> <destination ipv4 end>*}

Specifies the destination IPv4 address.

If `host` *<destination ipv4>* is specified, the flow detection condition is an exact match of *<destination ipv4>*.

To specify all destination IPv4 addresses, specify `any`. If `any` is specified, the destination IPv4 address is not used as a flow detection condition.

If `own-address` is specified, the IPv4 address that is set for the target interface is set for the flow detection conditions as the target IPv4 address.

If `own-prefix` is specified, the network address section of the IPv4 address that is set for the target interface is set for the flow detection conditions. The content of the host address section is user selectable.

If the interface where `own-address` and `own-prefix` are specified is multihomed, the primary IPv4 address is the target.

If `range-address` is specified, the flow detection condition is in the range from *<destination ipv4 start>* to *<destination ipv4 end>*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv4 address for *<destination ipv4>*.

   For *<destination ipv4 wildcard>*, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   Specify IPv4 addresses so that *<destination ipv4 end>* is larger than *<destination ipv4 start>*.

   IPv4 address (*nnn.nnn.nnn.nnn*): 0.0.0.0 to 255.255.255.255

{{eq | neq} *<destination port>* | range *<destination port start> <destination port end>*}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of *<destination port>*.

If `neq` is specified, the flow detection condition is other than *<destination port>*.

If `range` is specified, the flow detection condition is in the range from *<destination port start>* to *<destination port end>*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 3-4: Port names that can be specified for TCP* or *Table 3-5: Port names that can be specified for UDP (IPv4)*.

   Specify port numbers so that *<destination port end>* is larger than *<destination port start>*.

tos *<tos>*

Specifies 4 bits (bits 3 to 6) in the ToS field as the tos value.

The TOS value is compared with 4 bits (bits 3 to 6) in the ToS field of the sent or received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 3-7: tos names that can be specified*.

precedence <*precedence*>

Specifies the precedence value, which is the first 3 bits in the ToS field.

Its value is compared with the first 3 bits in the ToS field of the sent or received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 3-8: precedence names that can be specified*.

dscp <*dscp*>

Specifies the DSCP value, which is the first 6 bits in the ToS field.

Its value is compared with the first 6 bits in the ToS field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<icmp type>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp code>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp message>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be specified, see *Table 3-12: Message names that can be specified for ICMP (IPv4)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<igmp type>

Specifies the IGMP type.

This parameter option is available only if the protocol is IGMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

length {upper | lower} <*length*>

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of <*length*> or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of <*length*> or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

Specifies the MF flag value, which is the lower 1 bit in the Flags field.

`+mf` indicates a packet where an MF flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an MF flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

untagged

Specifies detection of untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

<*action specification*> parameter

action

Specifies the operation of the packet where a flow was detected. Specify the start of the entire <*action specification*> parameter.

1. Default value when this parameter is omitted:

   None (No operation is specified.)

2. Range of values:

   None

priority-class <*class*>

Specifies the priority class.

1. Default value when this parameter is omitted:

   None (The priority class is not changed.)

2. Range of values:

   Specify 1 to 8 in decimal.

discard-class <*class*>

Specifies the discard class.

The discard class of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

   None (The discard class is not changed.)

2. Range of values:

   Specify 1 to 4 in decimal.

replace-dscp <*dscp*>

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the <*dscp*> value.

1. Default value when this parameter is omitted:

   None. (The DSCP value is not replaced.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

replace-user-priority <*priority*>

Specifies the value for rewriting the user priority.

Replace the user priority of the received packet with <*priority*>.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

dscp-map

Enables DSCP mapping which determines the priority class and discard class based on the DSCP value.

For details on the priority class and discard class corresponding to the DSCP values, see the *6. Priority Change* in the manual *Configuration Guide Vol. 2 For Version 12.1*.

1. Default value when this parameter is omitted:

   None (DSCP mapping is not used.)

2. Range of values:

   None

policer <*policer name*>

Specifies the policer entry name.

1. Default value when this parameter is omitted:

   None (Policer function is not used.)

2. Range of values:

   Specifies the policer entry name that was set by the `policer` command.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `255.255.255.255` is entered for the source address wildcard mask and the destination address wildcard mask, `any` is displayed.
2. If `0.0.0.0` is entered for the source address wildcard mask and the destination address wildcard mask, `host` *nnn.nnn.nnn.nnn*, `host own-address` is displayed.

Related commands

```
ip qos-flow-list
ip qos-flow-group
ip qos-flow-list resequence
remark
policer
```

qos (ipv6 qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv6 QoS flow list.

If the `+fo` parameter is set for the flow detection conditions, the VLAN tag header conditions and IPv6 header conditions can be specified for the flow detection conditions. Layer 4 header conditions cannot be specified for the flow detection conditions.

Syntax

To set or change information:

```
[<sequence>] qos <target flow> [<action specification>]
```

To delete information:

```
no <sequence>
```

- *<target flow>*:

When the `+fo` parameter is not specified and the upper layer protocol is a type other than TCP, UDP, and ICMP:

```
{ipv6 | <protocol>} {<source ipv6>/<length> | host {<source ipv6> |
own-address} | any | own-address <own address length>} {<destination ipv6>/
<length>| host {<destination ipv6> | own-address} | any | own-address <own
address length> | own-prefix | range-address <destination ipv6 start>
<destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [-fo] [{untagged |
user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is TCP:

```
tcp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} [{{eq | neq} <source port> | range <source
port start> <source port end>}] {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{{eq | neq} <destination port> | range <destination port start> <destination
port end>}] [{[established] | [{+ack | -ack}] [{+fin | -fin}] [{+psh | -psh}]
[{+rst | -rst}] [{+syn | -syn}] [{+urg | -urg}]}] [{traffic-class <traffic
class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo]
[{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is UDP:

```
udp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} [{{eq | neq} <source port> | range <source
port start> <source port end>}] {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{{eq | neq} <destination port> | range <destination port start> <destination
port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [length {upper |
lower} <length>] [{+mf | -mf}] [-fo] [{untagged | user-priority <priority>}]
```

When the `+fo` parameter is not specified and the upper layer protocol is ICMP:

```
icmp {<source ipv6>/<length> | host {<source ipv6> | own-address} | any |
own-address <own address length>} {<destination ipv6>/<length>| host
{<destination ipv6> | own-address} | any | own-address <own address length>
| own-prefix | range-address <destination ipv6 start> <destination ipv6 end>}
[{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic
class> | dscp <dscp>}] [length {upper | lower} <length>] [{+mf | -mf}] [-fo]
[{untagged | user-priority <priority>}]
```

When the `+fo` parameter is specified:

```
{ipv6 | <protocol> | icmp | tcp | udp} {<source ipv6>/<length> | host {<source
ipv6> | own-address} | any | own-address <own address length>} {<destination
ipv6>/<length>| host {<destination ipv6> | own-address} | any | own-address
<own address length> | own-prefix | range-address <destination ipv6 start>
<destination ipv6 end>} [{traffic-class <traffic class> | dscp <dscp>}]
[length {upper | lower} <length>] [{+mf | -mf}] [+fo] [{untagged |
user-priority <priority>}]
```

- *<action specification>*:

  When no policer entry is included:

  ```
  action [replace-user-priority <priority>] [replace-dscp <dscp>]
  [{[priority-class <class>] [discard-class <class>] | dscp-map}]
  ```

  When a policer entry is included:

  ```
  action [policer <policer name>] [{priority-class <class> | dscp-map}]
  ```

Input mode

```
(config-ipv6-qos)
```

Parameters

<sequence>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the QoS flow list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<target flow> parameter

{ipv6 | *<protocol>* | icmp | tcp | udp}

Specifies the upper-layer protocol condition for IPv6 packets. Note that if all protocols are applicable, specify `ipv6`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 42, 45 to 49, 52 to 59, 61 to 255 (in decimal), or a protocol name.

   For details about the protocol names that can be specified, see *Table 3-3: Protocol names that can be specified (IPv6).*

{*<source ipv6>*/*<length>* | host {*<source ipv6>* | own-address} | any | own-address *<own address length>*}

Specifies the source IPv6 address.

If `host` *<source ipv6>* is specified, the flow detection condition is an exact match of *<source ipv6>*.

To specify all source IPv6 addresses, specify `any`. If `any` is specified, the source IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the source IPv6 address.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   Specify the source IPv6 address for <*source ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

   <*source ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <*length*>: 0 to 128

{{eq | neq} <*source port*> | range <*source port start*> <*source port end*>}

Specifies a source port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*source port*>.

If `neq` is specified, the flow detection condition is other than <*source port*>.

If `range` is specified, the flow detection condition is in the range from <*source port start*> to <*source port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 3-4: Port names that can be specified for TCP* or *Table 3-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*source port end*> is larger than <*source port start*>.

{<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own-prefix | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

If `host` <*destination ipv6*> is specified, the flow detection condition is an exact match of <*destination ipv6*>.

To specify all destination IPv6 addresses, specify `any`. If `any` is specified, the destination IPv6 address is not used as a flow detection condition.

If `own-address` is specified, the IPv6 global address that is set for the target interface is set for the flow detection conditions as the target IPv6 address.

If `own-prefix` is specified, the IPv6 global address that is set to the target interface is set for the flow detection conditions using the prefix length of the target IPv6 address and IPv6 global address for <*length*>.

If `range-address` is specified, the flow detection condition is in the range from <*destination ipv6 start*> to <*destination ipv6 end*>.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination IPv6 address for <*destination ipv6*>.

   For <*length*>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   For <*own address length*>, specify the part of the `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

   Specify IPv6 addresses so that <*destination ipv6 end*> is larger than <*destination ipv6 start*>.

   <*destination ipv6*> (*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*): 0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <*length*>: 0 to 128

{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}

Specifies the destination port number.

This parameter option is available only when the protocol is TCP or UDP.

If `eq` is specified, the flow detection condition is an exact match of <*destination port*>.

If `neq` is specified, the flow detection condition is other than <*destination port*>.

If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 (in decimal) or a port name.

   For details about the port names that can be set, see *Table 3-4: Port names that can be specified for TCP* or *Table 3-6: Port names that can be specified for UDP (IPv6)*.

   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

traffic-class <*traffic class*>

Specifies the traffic class field value.

Its value is compared with the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

dscp <*dscp*>

Specifies the DSCP value, which is the first 6 bits in the traffic class field.

Its value is compared with the first 6 bits in the traffic class field of the received packet.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

Specify 0 to 63 (in decimal) or the DSCP name.

For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

established

Specifies the detection of packets whose ACK flag or RST flag in the TCP header is 1.

This parameter option is available only when the protocol is TCP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+ack | -ack}

Specifies the detection of ACK flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+ack` indicates a packet where the ACK flag is 1, and `-ack` indicates a packet where the ACK flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fin | -fin}

Specifies the detection of FIN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+fin` indicates a packet where the FIN flag is 1, and `-fin` indicates a packet where the FIN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+psh | -psh}

Specifies the detection of PSH flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+psh` indicates a packet where the PSH flag is 1, and `-psh` indicates a packet where the PSH flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+rst | -rst}

Specifies the detection of RST flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+rst` indicates a packet where the RST flag is 1, and `-rst` indicates a packet where the RST flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+syn | -syn}

Specifies the detection of SYN flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+syn` indicates a packet where the SYN flag is 1, and `-syn` indicates a packet where the SYN flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+urg | -urg}

Specifies the detection of URG flags in the TCP header.

This parameter option is available only when the protocol is TCP.

`+urg` indicates a packet where the URG flag is 1, and `-urg` indicates a packet where the URG flag is 0.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

<*icmp type*>

Specifies the ICMP type.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<*icmp code*>

Specifies the ICMP code.

This parameter option is available only when the protocol is ICMP.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 255 in decimal.

<icmp message>

Specifies the ICMP message name.

This parameter option is available only when the protocol is ICMP.

For details about the ICMP message names that can be specified, see *Table 3-13: Message names that can be specified for ICMP (IPv6)*.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

length {upper | lower} *<length>*

Specifies the upper limit value or lower limit value of the IP user data length.

`upper`: Specifies the upper limit value. Packets with a length of *<length>* or less are set for the flow detection conditions.

`lower`: Specifies the lower limit value. Packets with a length of *<length>* or more are set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 65535 in decimal.

{+mf | -mf}

Specifies the M flag value of the fragment header.

`+mf` indicates a packet where an M flag of 1 is set for the flow detection conditions, and `-mf` indicates a packet where an M flag of 0 is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

{+fo | -fo}

Specifies the value of the Fragment Offset field.

`+fo` indicates a packet where a value other than 0 for the Fragment Offset field is set for the flow detection conditions, and `-fo` indicates a packet where a value of 0 for the Fragment Offset field is set for the flow detection conditions.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

untagged

Specifies detection of untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

<*action specification*> parameter

action

Specifies the operation of the packet where a flow was detected. Specify the start of the entire <*action specification*> parameter.

1. Default value when this parameter is omitted:

   None (No operation is specified.)

2. Range of values:

   None

priority-class <*class*>

Specifies the priority class.

1. Default value when this parameter is omitted:

   None (The priority class is not changed.)

2. Range of values:

   Specify 1 to 8 in decimal.

discard-class <*class*>

Specifies the discard class.

The discard class of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

   None (The discard class is not changed.)

2. Range of values:

   Specify 1 to 4 in decimal.

replace-dscp <*dscp*>

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the <*dscp*> value.

1. Default value when this parameter is omitted:

   None. (The DSCP value is not replaced.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

replace-user-priority <*priority*>

Specifies the value for rewriting the user priority.

Replace the user priority of the received packet with <*priority*>.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

dscp-map

Enables DSCP mapping which determines the priority class and discard class based on the DSCP value.

For details on the priority class and discard class corresponding to the DSCP values, see the *6. Priority Change* in the manual *Configuration Guide Vol. 2 For Version 12.1*.

1. Default value when this parameter is omitted:

   None (DSCP mapping is not used.)

2. Range of values:

   None

policer <*policer name*>

Specifies the policer entry name.

1. Default value when this parameter is omitted:

   None (Policer function is not used.)

2. Range of values:

   Specifies the policer entry name that was set by the policer command.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If 0 is entered for the <*length*> or <*own address length*> of the source address and destination address, `any` is displayed.
2. If 128 is entered for the <*length*> or <*own address length*> of the source address and destination address, `host` *nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*, `host own-address` is displayed.

Related commands

```
ipv6 qos-flow-list
ipv6 qos-flow-group
ipv6 qos-flow-list resequence
remark
policer
```

qos (mac qos-flow-list)

Specifies flow detection conditions and action specifications in the MAC QoS flow list.

Syntax

To set or change information:

```
[<sequence>] qos <target flow> [<action specification>]
```

To delete information:

```
no <sequence>
```

- <*target flow*>:

```
{<source mac> <source mac mask> | host <source mac> | any} {<destination mac>
<destination mac mask> | host <destination mac> | any | <destination mac name>}
[<ethernet type>] [{untagged | [user-priority <priority>] [tag-vlan <vlan id>]}]
```

- <*action specification*>:

When no policer entry is included:

```
action [replace-user-priority <priority>] [replace-dscp <dscp>]
[priority-class <class>] [discard-class <class>]
```

When a policer entry is included:

```
action [policer <policer name>] [priority-class <class>]
```

Input mode

```
(config-mac-qos)
```

Parameters

<*sequence*>

Specifies the sequence number for the order in which the flow detection conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the QoS flow list.

   If the condition is specified, this is the maximum value for the specified sequence number plus 10.

   Note, however, that if the maximum value for the sequence number is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<*target flow*> parameter

{<*source mac*> <*source mac mask*> | host <*source mac*> | any}

Specifies the source MAC address.

If `host` <*source mac*> is specified, the flow detection condition is an exact match of <*source mac*>.

To specify all source MAC addresses, specify `any`. If `any` is specified, the source MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Specify the source MAC address for <*source mac*>.

For <*source mac mask*>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | <*destination mac name*>}

Specifies the destination MAC address.

If `host` <*destination mac*> is specified, the flow detection condition is an exact match of <*destination mac*>.

To specify all destination MAC addresses, specify `any`. If `any` is specified, the destination MAC address is not used as a flow detection condition.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the destination MAC address for <*destination mac*>.

   For <*destination mac mask*>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   Specify the destination MAC address for <*destination mac name*>. For details about the destination MAC address names that can be specified, see *Table 3-11: Destination MAC address names that can be specified*.

   MAC address (*nnnn.nnnn.nnnn*): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<*ethernet type*>

Specifies the Ethernet type value.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name. For details about the Ethernet type names that can be specified, see *Table 3-10: Ethernet type names that can be specified*.

untagged

Specifies detection of untagged frames.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   None

user-priority <*priority*>

Specifies the user priority of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 7 in decimal.

tag-vlan <*vlan id*>

Specifies the VLAN ID of the first level VLAN tag.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 4095 in decimal.

<*action specification*> parameter

action

Specifies the operation of the packet where a flow was detected. Specify the start of the entire <*action specification*> parameter.

1. Default value when this parameter is omitted:

   None (No operation is specified.)

2. Range of values:

   None

priority-class <*class*>

Specifies the priority class.

1. Default value when this parameter is omitted:

   None (The priority class is not changed.)

2. Range of values:

   Specify 1 to 8 in decimal.

discard-class <*class*>

Specifies the discard class.

The discard class of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

   None (The discard class is not changed.)

2. Range of values:

   Specify 1 to 4 in decimal.

replace-dscp <*dscp*>

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the <*dscp*> value.

1. Default value when this parameter is omitted:

   None. (The DSCP value is not replaced.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see *Table 3-9: DSCP names that can be specified*.

replace-user-priority <*priority*>

Specifies the value for rewriting the user priority.

Replace the user priority of the received packet with <*priority*>.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

policer <*policer name*>

Specifies the policer entry name.

1. Default value when this parameter is omitted:

   None (Policer function is not used.)

2. Range of values:

   Specifies the policer entry name that was set by the `policer` command.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If *nnnn.nnnn.nnnn* `ffff.ffff.ffff` is entered as the source address and the destination address, `any` is displayed.
2. If the destination MAC address name or the address of the destination MAC address name is entered for the destination MAC address, the destination MAC address name is displayed.

   If *nnnn.nnnn.nnnn* `0000.0000.0000` is entered as the source address and the destination address in cases other than the above, `host` *nnnn.nnnn.nnnn* is displayed.

Related commands

```
mac qos-flow-list
mac qos-flow-group
mac qos-flow-list resequence
remark
policer
```

qos-queue-group

Sets the QoS queue list information for an Ethernet interface.

Syntax

To set information:

```
qos-queue-group <qos queue list name> out
```

To delete information:

```
no qos-queue-group
```

Input mode

`(config-if)`

Ethernet interface

Parameters

<qos queue list name>

Specifies the QoS queue list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   Specify a QoS queue list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

out

Specifies the sending side of the Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   None

Default behavior

PQ and number of queues operate at 8 in scheduling mode.

Impact on communication

If the QoS queue list name is specified and the number of queues is changed, all packets that have accumulated in the relevant queue are discarded.

When the change is applied

If the target Ethernet interface is in the normal operating state, after the setting value is changed, the changed value is immediately applied in operation. In other states, the setting value is applied when operation becomes the normal operating state.

Notes

1. If a QoS queue list name was specified that is not set by the `qos-queue-list` command, PQ and the number of queues operate at 8 in scheduling mode.
2. Only PQ and RR can be set for scheduling mode in 100GBASE-R Ethernet interfaces.

Related commands

```
qos-queue-list
interface gigabitethernet
interface tengigabitethernet
interface hundredgigabitethernet
```

qos-queue-list

Sets the scheduling mode and number of queues for the QoS queue list information.

Syntax

To set or change information:

```
qos-queue-list <qos queue list name> { pq [{ number_of_queue_1 |
number_of_queue_2 | number_of_queue_4 }] | rr [{ number_of_queue_1 |
number_of_queue_2 | number_of_queue_4 }] | 4pq+4wfq <rate1>% <rate2>%
<rate3>% <rate4>% | 2pq+4wfq+2beq <rate3>% <rate4>% <rate5>% <rate6>% |
4wfq+4beq <rate5>% <rate6>% <rate7>% <rate8>% }
```

To delete information:

```
no qos-queue-list <qos queue list name>
```

Input mode

```
(config)
```

Parameters

<qos queue list name>

Specifies the QoS queue list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a QoS queue list name with no more than 31 characters.

   For details, see *Specifiable values for parameters*.

{ pq [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }] | rr [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }] | 4pq+4wfq *<rate1>*% *<rate2>*% *<rate3>*% *<rate4>*% | 2pq+4wfq+2beq *<rate3>*% *<rate4>*% *<rate5>*% *<rate6>*% | 4wfq+4beq *<rate5>*% *<rate6>*% *<rate7>*% *<rate8>*% }

Specifies the scheduling mode. The number of queues can be selected from a fixed 8 queues or from 1, 2, 4, or 8 queues based on the scheduling mode. The priority of queues for PQ operation is higher for larger queue numbers.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

pq [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }]

The PQ scheduling mode is used. Also, sets the number of queues per Ethernet interface.

The number of queues can be selected as 1, 2, or 4 queues per Ethernet interface, and it is set to 8 queues if nothing is selected.

number_of_queue_1: Number of queues is 1.

number_of_queue_2: Number of queues is 2.

number_of_queue_4: Number of queues is 4.

1. Default value when this parameter is omitted:

   If `pq` only is specified, the number of queues is 8.

rr [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }]

The PR scheduling mode is used. Also, sets the number of queues per Ethernet interface.

The number of queues can be selected as 1, 2, or 4 queues per Ethernet interface, and it is set to 8 queues if nothing is selected.

number_of_queue_1: Number of queues is 1.

number_of_queue_2: Number of queues is 2.

number_of_queue_4: Number of queues is 4.

1. Default value when this parameter is omitted:

   If `rr` only is specified, the number of queues is 8.

4pq+4wfq *<rate1>*% *<rate2>*% *<rate3>*% *<rate4>*%

Operates at 4PQ+4WFQ. The number of queues is fixed at 8 queues per Ethernet interface. 4wfq sends packets based on the weight ratio <*rate*> that was set. The number added to the end of <*rate*> indicates the queue number.

1. Default value when this parameter is omitted:

   <*rate*>: This parameter cannot be omitted.

2. Range of values:

   <*rate*>: 1 to 97

   Notes: Make the settings so that the equations below are satisfied.

   * *<rate1>* + *<rate2>* + *<rate3>* + *<rate4>* = 100

   * *<rate1>* ≤ *<rate2>* ≤ *<rate3>* ≤ *<rate4>*

2pq+4wfq+2beq *<rate3>*% *<rate4>*% *<rate5>*% *<rate6>*%

Operates at 2PQ+4WFQ+2BEQ. The number of queues is fixed at 8 queues per Ethernet interface. 4wfq sends packets based on the weight ratio <*rate*> that was set. The number added to the end of <*rate*> indicates the queue number.

1. Default value when this parameter is omitted:

   <*rate*>: This parameter cannot be omitted.

2. Range of values:

   <*rate*>: 1 to 97

   Notes: Make the settings so that the equations below are satisfied.

   * *<rate3>* + *<rate4>* + *<rate5>* + *<rate6>* = 100

   * *<rate3>* ≤ *<rate4>* ≤ *<rate5>* ≤ *<rate6>*

4wfq+4beq *<rate5>*% *<rate6>*% *<rate7>*% *<rate8>*%

Operates at 4WFQ+4BEQ. The number of queues is fixed at 8 queues per Ethernet interface. 4wfq sends packets based on the weight ratio <*rate*> that was set. The number added to the end of <*rate*> indicates the queue number.

1. Default value when this parameter is omitted:

   <*rate*>: This parameter cannot be omitted.

2. Range of values:

   <*rate*>: 1 to 97

   Notes: Make the settings so that the equations below are satisfied.

   * *<rate5>* + *<rate6>* + *<rate7>* + *<rate8>* = 100

   * *<rate5>* ≤ *<rate6>* ≤ *<rate7>* ≤ *<rate8>*

Default behavior

None

Impact on communication

If the QoS queue list name is specified for the `qos-queue-group` command and the number of queues is changed, all packets that have accumulated in the relevant queue are discarded.

When the change is applied

If the Ethernet interface where the QoS queue list information is applied is in the normal operating state, after the setting value is changed, the changed value is immediately applied in operation. In other states, the setting value is applied when operation becomes the normal operating state.

Notes

1. PQ and RR only can be set for scheduling mode in 100GBASE-R Ethernet interfaces.
2. If the scheduling mode and number of queues are changed, the statistics displayed for the `show qos queueing port` operation command and the axPortOutQueue group in the relevant Ethernet interface are cleared to 0.

Related commands

`qos-queue-group`

remark

Sets supplementary information for a QoS flow list.

IPv4 QoS flow list, IPv6 QoS flow list, MAC QoS flow list, and Advance QoS flow list are available as QoS flow list.

Syntax

To set or change information:

```
remark <remark>
```

To delete information:

```
no remark
```

Input mode

```
(config-ip-qos)
(config-ipv6-qos)
(config-mac-qos)
(config-adv-qos)
```

Parameters

<remark>

Sets supplementary information about the applicable QoS flow list depending on input mode.

Only one line can be set for one QoS flow list. Entering new information overwrites the existing information.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify a character string with no more than 64 characters. Enclose it in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
advance qos-flow-list
ip qos-flow-list
ipv6 qos-flow-list
mac qos-flow-list
```

traffic-shape rate

Sets port bandwidth control for an Ethernet interface.

Syntax

To set or change information:

```
    traffic-shape rate {<kbit/s>k | <Mbit/s>M | <Gbit/s>G}
```

To delete information:

```
    no traffic-shape rate
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

rate {<*kbit/s*>k | <*Mbit/s*>M | <*Gbit/s*>G}

Sets port bandwidth control.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See the table below.

   You can specify k, M, or G for the unit of the value. k indicates 1000, M indicates 1000^2, and G indicates 1000^3.

Table 3-14: Setting range for port bandwidth control

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

Default behavior

Operation is at line speed.

Impact on communication

Traffic might flow temporarily at line speed until the setting of the port bandwidth control is complete.

When the change is applied

If the target Ethernet interface is in the normal operating state, after the setting value is changed, the changed value is immediately applied in operation. In other states, the setting value is applied when operation enters the normal operating state.

Notes

1. If the line state is half duplex, data might be unable to be sent up to the bandwidth that was set in port bandwidth control.

Related commands

```
interface gigabitethernet
interface tengigabitethernet
interface hundredgigabitethernet
```

Chapter

4. Port Mirroring

monitor session

monitor session

Configures the port mirroring functionality.

Syntax

To set information:

```
monitor session <session no.> source interface <interface id list> {rx | tx
| both} destination interface {gigabitethernet | tengigabitethernet |
hundredgigabitethernet} <nif no.>/<port no.>
```

To change information:

```
monitor session <session no.> source interface <interface id list> {rx | tx
| both} destination interface {gigabitethernet | tengigabitethernet |
hundredgigabitethernet} <nif no.>/<port no.>
monitor session <session no.> { source interface add <interface id list> |
source interface remove <interface id list> }
```

To delete information:

```
no monitor session <session no.>
```

Input mode

`(config)`

Parameters

<session no.>

Specifies a port mirroring session number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1000

source interface *<interface id list>*

Specify a monitor port for port mirroring in list format.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

source interface add *<interface id list>*

Adds a monitor port for port mirroring to the list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

source interface remove *<interface id list>*

Deletes a monitor port for port mirroring from the list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

{rx | tx | both}

Specifies the direction of the traffic subject to port mirroring.

rx

Received frames are mirrored.

tx

Sent frames are mirrored.

both

Both sent and received frames are mirrored.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

destination interface {gigabitethernet | tengigabitethernet | hundredgigabitethernet} *<nif no.>/<port no.>*

Specifies a mirror port for port mirroring.

{gigabitethernet | tengigabitethernet | hundredgigabitethernet}

Specifies the mirror port type.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<nif no.>/<port no.>

Specifies the NIF number and the port number for the mirror port.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One mirror port can be set for multiple monitor ports. Incoming frames that were copied by port mirroring cannot be sent to multiple mirror ports, and outgoing frames that were copied

cannot be sent to multiple mirror ports.

2. If the number of frames copied by port mirroring exceeds the line bandwidth, the frames are discarded.
3. A port that has already been set as a mirror port cannot be set as a monitor port.
4. If the configuration for an interface that was set for the monitor port or mirror port is deleted, the configuration of the port mirroring session that includes the relevant port is also deleted. If a port list is specified for a monitor port, and one of the above types of port is in the port list, the corresponding port mirroring session will be deleted.

Related commands

None

Chapter

5. sFlow Statistics

sflow additional-http-port
sflow destination
sflow extended-information-type
sflow forward ingress
sflow max-header-size
sflow max-packet-size
sflow packet-information-type
sflow polling-interval
sflow sample
sflow source

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.

Syntax

To set or change information:

```
    sflow additional-http-port <HTTP port>
```

To delete information:

```
    no sflow additional-http-port
```

Input mode

```
(config)
```

Parameters

<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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

The port number used for HTTP packets is set to 80 only.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow destination

Specifies the IP address of the collector, which is the destination for sFlow packets.

Syntax

To set information:

```
sflow destination { <ip address> | <ipv6 address> } [<udp port>]
```

To delete information:

```
no sflow destination { <ip address> | <ipv6 address> } [<udp port>]
```

Input mode

```
(config)
```

Parameters

{ <ip address> | <ipv6 address> }

Specifies the IP address of the collector, which is the destination for sFlow packets. A maximum of four sets of the IP address and UDP port can be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify IP addresses in IPv4 or IPv6 format.

<udp port>

Specifies the UDP port number of the collector, which is the destination for sFlow packets.

1. Default value when this parameter is omitted:

   6343

2. Range of values:

   0 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This parameter cannot be changed. First delete the parameter, and then add it again.
2. You can set multiple UDP port numbers for an IP address.
3. The broadcast address, multicast address, and link-local address cannot be set for the IPv4 and IPv6 addresses of the collector.

Related commands

None

sflow extended-information-type

Sets whether to send flow samples in an extended data format.

Syntax

To set or change information:

```
sflow extended-information-type { [router] [gateway] [user] [url] | none }
```

To delete information:

```
no sflow extended-information-type
```

Input mode

```
(config)
```

Parameters

{ [router] [gateway] [user] [url] | none }

Sets whether to send flow samples in an extended data format.

The extended data format to be specified here is a set of network information, such as information related to switches or routers, that can be judged from packet information. For details, see *10.1.3(2)(c) Extended data format* in the manual *Configuration Guide Vol. 2 For Version 12.1*.

You can specify this parameter multiple times. When you specify multiple parameters, separate pairs of parameters with a space character. However, note that you cannot specify any other parameters together with the `none` parameter.

router

Enables the sending of router information (such as NextHop).

gateway

Enables the sending of gateway information (such as the AS number).

user

Enables the sending of user information (such as TACACS or RADIUS information).

url

Enables the sending of URL information.

none

No flow samples in any extended data format are to be sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Flow samples in any extended data format are sent to the collector.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Any new setting of this command overwrites the old setting. If you want to change a parameter, enter all the necessary parameter values at the same time when you set this command.

Related commands

None

sflow forward ingress

The incoming traffic of the specified port is sampled for flow samples, and the outgoing and incoming traffic is monitored for counter samples.

Syntax

To set information:

```
sflow forward ingress
```

To delete information:

```
no sflow forward ingress
```

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow max-header-size

Sets the maximum size from the beginning of the sample packet (beginning of MAC header) to be copied, if the header type is used for the basic data format (see the `sflow packet-information-type` command).

Syntax

To set or change information:

```
sflow max-header-size <bytes>
```

To delete information:

```
no sflow max-header-size
```

Input mode

```
(config)
```

Parameters

<bytes>

If the header type is used for the basic data format, this parameter sets the maximum size to be copied (in bytes), starting from the beginning of the sample packet (beginning of MAC header).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 256

Default behavior

A maximum of 128 bytes are copied from the beginning of the sample packet (beginning of MAC header).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow max-packet-size

Specifies the maximum size of an sFlow packet. The specified size is the length from the sFlow header to the end of the packet.

Syntax

To set or change information:

```
sflow max-packet-size <bytes>
```

To delete information:

```
no sflow max-packet-size
```

Input mode

```
(config)
```

Parameters

<bytes>

Specifies the maximum size of an sFlow packet (in bytes). Specify a value equal to or smaller than the MTU length value (in bytes) set to the source interface from which the sFlow packet is to be sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1400 to 9216

Default behavior

The maximum size of an sFlow packet is 1400 bytes.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow packet-information-type

Sets the basic data format of the flow sample.

Syntax

To set information:

```
sflow packet-information-type ip
```

To delete information:

```
no sflow packet-information-type
```

Input mode

```
(config)
```

Parameters

ip

Sets the basic data format of the flow sample.

When `ip` has been specified, flow samples are sent to the collector in IPv4 format if the applicable packet is an IPv4 packet, or in IPv6 format if the applicable packet is an IPv6 packet. For details about the basic data format specified here, see *10.1.3(2)(b) Basic data format* in the manual *Configuration Guide Vol. 2 For Version 12.1*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Flow samples are sent to the collector in header type format.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow polling-interval

Specifies the interval for sending counter samples to the collector.

Syntax

To set or change information:

```
    sflow polling-interval <seconds>
```

To delete information:

```
    no sflow polling-interval
```

Input mode

```
(config)
```

Parameters

<seconds>

Specifies the interval for sending counter samples to the collector (in seconds). If 0 second is specified, counter samples are not sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 2147483647 (= 2^31 - 1)

Default behavior

Counter samples are sent to the collector in every 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If 20 or more ports are monitored, the load on the Device might be excessive. In such a case, as the guideline, specify an interval value (in seconds) equal to the total number of monitored physical ports.

   Example: If there are 40 monitored physical ports, specify 40 seconds or more for the interval value.

Related commands

None

sflow sample

Specifies the sampling interval applying to the Device.

Syntax

To set or change information:

```
sflow sample <sample count>
```

To delete information:

```
no sflow sample
```

Input mode

```
(config)
```

Parameters

<sample count>

Specifies the sampling interval (in the unit of packets) that applies to the Device. The sampling probability is one packet (sampled) per sampling interval. For example, if the sampling interval is set to 512, the probability of a packet being sampled is one in 512.

Use the `show interfaces` operation command to check all the received and sent packet flow rates (packets per second) from the operating status of the port where sFlow statistics are to be enabled. The recommended value is described in the *Sampling interval to be used as a guideline* column for the applicable total packet flow rate (packets per second) in *Table 5-1: Sampling interval to be used as a guideline in an operating environment*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1, 2, 8, 32, 128, 512, 2048, 8192, 32768, 131072, 524288, 2097152, 8388608, 33554432, 134217728, and 536870912

   Specify 1, or a value that can be obtained from (2 x 4^n), where n = 0 to 14. If a value other than these values is entered, one of these values is automatically set depending on the entered value. *Table 5-2: Relationship between the entered sampling interval and the sampling interval that is actually set* describes the relationship between the entered value and set value.

Table 5-1: Sampling interval to be used as a guideline in an operating environment

Total packet flow rate (packets per second)	Sampling interval to be used as a guideline	Example implementation to be used as a guideline
Up to 8 kpacket/s	8	
Up to 32 kpacket/s	32	
Up to 128 kpacket/s	128	100 Mbit/s Ethernet x 1
Up to 512 kpacket/s512	512	
Up to 2 Mpacket/s	2048	1 Gbit/s Ethernet x 1
Up to 8 Mpacket/s	8192	10 Gbit/s Ethernet x 1
Up to 32 Mpacket/s	32768	
Up to 128 Mpacket/s	131072	10 Gbit/s Ethernet x 480

Total packet flow rate (packets per second)	Sampling interval to be used as a guideline	Example implementation to be used as a guideline
Up to 512 Mpacket/s	524288	100 Gbit/s Ethernet x 8
Up to 1.6 Gpacket/s	2097152	100 Gbit/s Ethernet x 16

Table 5-2: Relationship between the entered sampling interval and the sampling interval that is actually set

Sampling interval entered in the command	Sampling interval actually set
1	1
2	2
3 to 8	8
9 to 32	32
33 to 128	128
129 to 512	512
513 to 2048	2048
2049 to 8192	8192
8193 to 32768	32768
32769 to 131072	131072
131073 to 524288	524288
524289 to 2097152	2097152
2097153 to 8388608	8388608
8388609 to 33554432	33554432
33554433 to 134217728	134217728
134217729 to 536870912	536870912

Example:

If 1000 is specified for <*sample count*>, the value that is actually used is 2048 (= 2 x 4^5).

Default behavior

The sampling interval applied to the Device is 536870912 (= 2 x 4^14).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a sampling interval is set that is shorter than the recommended value shown in *Sampling interval to be used as a guideline* in *Table 5-1: Sampling interval to be used as a guideline in an operating environment*, make sure that you set a sampling interval after first fully verifying device operation, including the operation of other functions.

Related commands

None

sflow source

Specifies the IP address to be configured as the sFlow packet source (agent).

Syntax

To set or change information:

```
sflow source { <ip address> | <ipv6 address> }
```

To delete information:

```
no sflow source { <ip address> | <ipv6 address> }
```

Input mode

```
(config)
```

Parameters

{ *<ip address>* | *<ipv6 address>* }

Specifies the IP address to be used as the sFlow packet source (agent). You can specify one IPv4 address or one IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify IP addresses in IPv4 or IPv6 format.

Default behavior

If this command is not specified, the IP address is set according to the priorities below. Similarly, if the specified IP address format is different from the address type specified in the `sflow destination` command, the IP address is set according to the following priorities.

Priority 1

The loopback interface address (when a loopback interface address has been set by the configuration command)

Priority 2

An IP address is automatically assigned from the IP address assigned to an interface of the Device.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The broadcast address, multicast address, and link-local address cannot be set for the agent IP address of sFlow packets.
2. For the IP address to be used as the agent IP address, specify the IP address assigned to an interface of the Device. If the specified IP address is not the one set for the Device, sFlow packets cannot be sent.

Related commands

None

Chapter

6. CFM

cc alarm-priority
cc alarm-reset-time
cc alarm-start-time
cc cos
cc enable
cc interval
domain-name
ethernet cfm ais enable
ethernet cfm cc cos
ethernet cfm domain-level
ethernet cfm enable (global)
ethernet cfm enable (interface)
ethernet cfm lck enable
ethernet cfm mel
ethernet cfm mep
ma-id
meg-id

cc alarm-priority

Sets the failure level detected by the CC functionality. A failure that exceeds the set failure level is to be detected.

Syntax

To set or change information:

```
cc alarm-priority <priority>
```

To delete information:

```
no cc alarm-priority
```

Input mode

```
(config-ether-cfm)
```

Parameters

<priority>

Sets the lowest failure level that will be detected by CC.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 5

   The following table describes the failure descriptions corresponding to the setting values.

Table 6-1: Failure descriptions corresponding to the setting values

Value set	Failure type	Display in a command	Problem
0	none	--	No failure was detected.
1	DefRDICCM	RDI	A CCM with the failure flag on was received.
2	DefMACstatus	PortState	A received CCM has information about whether a port or interface is in the down state.
3	DefRemoteCCM	Timeout	A CCM from a remote MEP has timed out.
4	DefErrorCCM	ErrorCCM	A MEP configuration error occurred, or a CCM with an abnormal sending interval was received.
5	DefXconCCM	OtherCCM	A CCM with a different MA was received.

Legend: --: Not applicable

Default behavior

Level 2 or higher failures are detected.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
cc enable
```

cc alarm-reset-time

If CC detects repeated failures, this sets the time interval within which the CC functionality recognizes that this is a redetected failure. After detecting a failure, if another failure is detected within the time interval set by using this command, the failure is treated as a redetected failure and no trap is sent. However, if the level of the redetected failure is higher than that of the previously-detected failure, a trap is sent.

Syntax

To set or change information:

```
cc alarm-reset-time <time>
```

To delete information:

```
no cc alarm-reset-time
```

Input mode

```
(config-ether-cfm)
```

Parameters

<time>

Sets the period of time until the CC functionality recognizes that the failure is a redetected failure. The actual value used is set in 500 millisecond increments (a value less than 500 milliseconds is rounded up to 500 milliseconds).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2500 to 10000 (milliseconds)

Default behavior

The period of time until the CC functionality recognizes that the failure is a redetected failure is set to 10000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
cc enable
```

cc alarm-start-time

Sets the time from the point at which CC detects a failure until it sends a trap.

Syntax

To set or change information:

```
cc alarm-start-time <time>
```

To delete information:

```
no cc alarm-start-time
```

Input mode

```
(config-ether-cfm)
```

Parameters

<time>

Sets the time delay from when CC detects a failure until CC sends a trap. The actual value used is set in 500 millisecond increments (a value less than 500 milliseconds is rounded up to 500 milliseconds).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2500 to 10000 (milliseconds)

Default behavior

After detection of a failure, there is a time delay of 2500 milliseconds until a trap is sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
cc enable
```

cc cos

Sets the CoS value when sending CCMs.

Syntax

To set or change information:

```
cc cos <cos>
```

To delete information:

```
no cc cos
```

Input mode

```
(config-ether-cfm)
```

Parameters

<cos>

Specifies the CoS value when sending CCMs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

Default behavior

A CoS value of 7 is used for operation.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The value of this command is not applied to the MA and MEG that are used to set the `ethernet cfm cc cos` command.

Related commands

```
cc enable
```

cc enable

MA or MEG are used to enable CC.

If the `ethernet cfm mep` command has already been set, sending from the applicable port to CCM starts.

Syntax

To set information:

```
    cc enable
```

To delete information:

```
    no cc enable
```

Input mode

```
(config-ether-cfm)
```

Parameters

None

Default behavior

Monitoring by CC and CCM sending are not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
ethernet cfm mep
```

cc interval

Sets the CCM transmission interval for a target MA or MEG.

Syntax

To set or change information:

```
    cc interval {1sec | 10sec | 1min | 10min}
```

To delete information:

```
    no cc interval
```

Input mode

```
(config-ether-cfm)
```

Parameters

{1sec | 10sec | 1min | 10min}

Sets the interval for sending CCMs.

1sec

Sets the interval for sending CCMs to 1 second.

10sec

Sets the interval for sending CCMs to 10 seconds.

1min

Sets the interval for sending CCMs to 1 minute.

10min

Sets the interval for sending CCMs to 10 minutes.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`1min` is used as the interval for sending CCMs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the interval for sending CCMs is set to a shorter value than the initial value, the CPU usage of the device becomes higher, which might affect communication.

Related commands

```
cc enable
```

domain-name

Sets the name used for a domain.

Syntax

To set or change information:

```
domain-name {no-present | str <string> | dns <name> | mac <mac> <id>}
```

To delete information:

```
no domain-name
```

Input mode

```
(config-ether-cfm)
```

Parameters

{no-present | str <*string*> | dns <*name*> | mac <*mac*> <*id*>}

Sets the parameter to be used as the domain name.

no-present

If this parameter is set, the Maintenance Domain Name field in CCM is not used.

str <*string*>

Uses a character string of no more than 43 characters to specify a domain name.

dns <*name*>

Uses the domain name server name as the domain name.

mac <*mac*> <*id*>

Uses the MAC address and a 2-byte ID as a domain name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*string*>, enclose a character string consisting of no more than 43 characters in double quotation marks. Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

   For <*name*>, specify a host name with no more than 63 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

   For <*mac*>, specify a value from `0000.0000.0000` to `feff.ffff.ffff`. Note that you cannot specify a multicast MAC address (address in which the lowest bit of the first byte is 1).

   For <*id*>, specify a value from 0 to 65535.

Default behavior

The Maintenance Domain Name field in CCM is not used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When a parameter other than `no-present` has been specified, if a character string with more than 43 characters is specified for the `str` <*string*> parameter in the `ma-id` command, the first character of the specified parameter is added to CCM.

Related commands

None

ethernet cfm ais enable

The `no ethernet cfm ais enable` command disables ETH-AIS for the relevant port or port channel.

Syntax

To set information:

```
no ethernet cfm ais enable
```

To delete information:

```
ethernet cfm ais enable
```

Input mode

`(config-if)`

Ethernet interface or port channel interface

Parameters

None

Default behavior

Enables ETH-AIS.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

`ethernet cfm mel`

ethernet cfm cc cos

Sets the CoS value when sending CCMs for MEP.

Syntax

To set or change information:

```
ethernet cfm cc domain-level <level> ma <no.> mep-id <mepid> cos <cos>
ethernet cfm cc mel <level> meg <no.> mep-id <mepid> cos <cos>
```

To delete information:

```
no ethernet cfm cc domain-level <level> ma <no.> mep-id <mepid> cos
no ethernet cfm cc mel <level> meg <no.> mep-id <mepid> cos
```

Input mode

`(config-if)`

Ethernet interface or port channel interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

domain-level <*level*> (IEEE 802.1ag standard)

Specifies the level that was set by using the `ethernet cfm domain-level` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*> (IEEE 802.1ag standard)

Specifies the MA ID number that was set by using the `ethernet cfm domain-level` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

mel <*level*> (ITU-T Y.1731 standard)

Specifies the level that was set by using the `ethernet cfm mel` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

meg <*no.*> (ITU-T Y.1731 standard)

Specifies the MEG ID number that was set by using the `ethernet cfm mel` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

mep-id <*mepid*>

Specify a MEP ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   1 to 8191

<*cos*>

Specifies the CoS value when sending CCMs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   0 to 7

Default behavior

The setting of the `cc cos` command is used. If the `cc cos` command is not set, a CoS value of 7 is used for operation.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

`cc enable`

ethernet cfm domain-level

Sets the domain and MA. Executing this command changes the mode to the mode for setting CFM.

Syntax

To set information:

```
ethernet cfm domain-level <level> ma <no.>
```

To delete information:

```
no ethernet cfm domain-level <level> ma <no.>
```

Input mode

```
(config)
```

Parameters

<level>

Specifies the level.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma *<no.>*

Specifies the MA ID number.

The same value as the MEG identification number that was already set by the `ethernet cfm mel` command cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `ethernet cfm mep` command references a domain set by using this command, this command cannot be deleted.

Related commands

```
cc enable
ethernet cfm mep
```

ethernet cfm enable (global)

Starts CFM.

Syntax

To set information:

```
    ethernet cfm enable
```

To delete information:

```
    no ethernet cfm enable
```

Input mode

```
(config)
```

Parameters

None

Default behavior

CFM does not operate even if another CFM command has been set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

ethernet cfm enable (interface)

The `no ethernet cfm enable` command stops the CFM PDU send or receive process for the relevant port or port channel.

Syntax

To set information:

```
no ethernet cfm enable
```

To delete information:

```
ethernet cfm enable
```

Input mode

`(config-if)`

Ethernet interface or port channel interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

None

Default behavior

CFM PDUs can be received.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

None

ethernet cfm lck enable

The `no ethernet cfm lck enable` command disables ETH-LCK for the relevant port or port channel.

Syntax

To set information:

```
no ethernet cfm lck enable
```

To delete information:

```
ethernet cfm lck enable
```

Input mode

```
(config-if)
```

Ethernet interface or port channel interface

Parameters

None

Default behavior

Enables ETH-LCK.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

```
ethernet cfm mel
```

ethernet cfm mel

Sets the MEG. Executing this command changes the mode to the mode for setting CFM.

Syntax

To set information:

```
ethernet cfm mel <level> meg <no.>
```

To delete information:

```
no ethernet cfm mel <level> meg <no.>
```

Input mode

```
(config)
```

Parameters

<level>

Specifies the level.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

meg *<no.>*

Specifies the MEG ID number.

The same value as the MA identification number that was already set by the `ethernet cfm domain-level` command cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `ethernet cfm mep` command references a MEG set by using this command, this command cannot be deleted.

Related commands

```
cc enable
ethernet cfm mep
```

ethernet cfm mep

Sets an MEP used by the CFM functionality.

Syntax

To set information:

```
ethernet cfm mep domain-level <level> ma <no.> mep-id <mepid>
ethernet cfm mep mel <level> meg <no.> mep-id <mepid>
```

To delete information:

```
no ethernet cfm mep domain-level <level> ma <no.> mep-id <mepid>
no ethernet cfm mep mel <level> meg <no.> mep-id <mepid>
```

Input mode

`(config-if)`

Ethernet interface or port channel interface

`(config-subif)`

Ethernet subinterface or port channel subinterface

Parameters

domain-level <*level*> (IEEE 802.1ag standard)

Specifies the level that was set by using the `ethernet cfm domain-level` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*> (IEEE 802.1ag standard)

Specifies the MA ID number that was set by using the `ethernet cfm domain-level` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

mel <*level*> (ITU-T Y.1731 standard)

Specifies the level that was set by using the `ethernet cfm mel` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

meg <no.> (ITU-T Y.1731 standard)

Specifies the MEG ID number that was set by using the `ethernet cfm mel` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

mep-id <*mepid*>

Specify a MEP ID. Set a value unique within the MA or MEG.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8191

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

None

ma-id

Sets the name of an MA used for the applicable domain.

Syntax

To set or change information:

```
    ma-id {str <string> | vlan <vlan id>}
```

To delete information:

```
    no ma-id
```

Input mode

```
(config-ether-cfm)
```

Parameters

{str <*string*> | vlan <*vlan id*>}

Specifies the name of an MA by using a character string or a VLAN ID.

str <*string*>

A character string specified for <*string*> is used for the name of an MA.

vlan <*vlan id*>

The VLAN ID specified for <*vlan id*> is used as the name of the MA.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*string*>, enclose a character string consisting of no more than 45 characters in double quotation marks. Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

   Specify a value from 1 to 4095 for <*vlan id*>.

Default behavior

The value specified for the `ma` parameter using the `ethernet cfm domain-level` command is used for the MA name.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a parameter other than `no-present` has been set by using the `domain-name` command and you specify a character string of 44 characters or more for <*string*>, the 44th and subsequent characters are not used in the Short MA Name field in the CCM.
2. <*string*> or <*vlan id*> that has already been set in the same domain cannot be specified.

Related commands

```
ethernet cfm domain-level
```

meg-id

Sets the MEG ID used for the relevant MEG.

Syntax

To set or change information:

```
meg-id icc <string> umc <string>
```

To delete information:

```
no meg-id
```

Input mode

```
(config-ether-cfm)
```

Parameters

icc <*string*>

Specifies the character string used for the ITU carrier code (ICC).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 6 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

umc <*string*>

Specifies the character string used for the unique MEG ID code (UMC).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 6 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The value specified for the `meg` parameter using the `ethernet cfm mel` command is used for the MEG ID.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. ICC and UMC combinations that were already set in the same MEG level cannot be specified.
2. If the total of the character string length specified by the parameters `icc` and `umc` is less than

6 characters, the remaining fields that are set for the MEG ID are NULL.

Related commands

```
ethernet cfm mel
```

Chapter

7. LLDP

lldp enable
lldp hold-count
lldp interval-time
lldp run

lldp enable

Enables operation of LLDP for a port.

Syntax

To set information:

```
lldp enable
```

To delete information:

```
no lldp enable
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
lldp run
```

lldp hold-count

Specifies the scaling for the value specified by the `lldp interval-time` command as the time that a neighboring device retains the LLDP frame sent from the Device.

Syntax

To set or change information:

```
lldp hold-count <count>
```

To delete information:

```
no lldp hold-count
```

Input mode

```
(config)
```

Parameters

<count>

Specifies the scaling for the time period that a neighboring device retains the LLDP frame. If the period exceeds 65535 (seconds), which is the maximum value, 65535 (seconds) is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2 to 10

Default behavior

4 is set as the period that a neighboring device retains LLDP frames.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
lldp run
```

lldp interval-time

Specifies the interval at which the Device sends LLDP frames.

Syntax

To set or change information:

```
lldp interval-time <seconds>
```

To delete information:

```
no lldp interval-time
```

Input mode

```
(config)
```

Parameters

<seconds>

Specifies the transmission interval (in seconds) between LLDP frames sent from the Device.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   5 to 32768

Default behavior

30 seconds is used as the sending interval between LLDP frames sent from the Device.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

```
lldp run
```

lldp run

Enables the LLDP functionality.

Syntax

To set information:

```
lldp run
```

To delete information:

```
no lldp run
```

Input mode

```
(config)
```

Parameters

None

Default behavior

The LLDP functionality is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

Chapter

8. Error Messages Displayed When Editing the Configuration

8.1 Common errors
8.2 Errors when specifying access list settings
8.3 Errors when specifying QoS settings
8.4 Errors when specifying port mirroring settings
8.5 Errors when specifying CFM settings
8.6 Errors when specifying LLDP settings

8.1 Common errors

For details about error messages common to all functionality, see the manual *17.1 Common errors* in the manual *Configuration Command Reference Vol. 1 For Version 12.1*.

8.2 Errors when specifying access list settings

Table 8-1: Error messages displayed when specifying access list settings

Message	Description
The IPv4 policy-based routing entry cannot be set because the specified destination IPv4 address is invalid.	The entry cannot be set because the destination IPv4 address specified as a flow detection condition is not supported by IPv4 policy-based routing. If IPv4 policy-based routing is specified, specify addresses other than those shown below for the destination IPv4 address. • Multicast addresses • Conditional broadcast addresses • `host own-address` parameter Also, an IPv4 address that is set to a target interface cannot be specified.
The IPv4 policy-based routing entry cannot be set because the specified source IPv4 address is invalid.	The entry cannot be set because the source IPv4 address specified as a flow detection condition is not supported by IPv4 policy-based routing. If IPv4 policy-based routing is specified, specify IPv4 addresses other than multicast addresses for the source IPv4 addresses.
The IPv6 policy-based routing entry cannot be set because the specified destination IPv6 address is invalid.	The entry cannot be set because the destination IPv6 address specified as a flow detection condition is not supported by IPv6 policy-based routing. If IPv6 policy-based routing is specified, specify addresses other than those shown below for the destination IPv6 address. • Multicast addresses • Link-local address • `host own-address` parameter Also, an IPv6 address that is set to a target interface cannot be specified.
The IPv6 policy-based routing entry cannot be set because the specified source IPv6 address is invalid.	The entry cannot be set because the source IPv6 address specified as a flow detection condition is not supported by IPv6 policy-based routing. If IPv6 policy-based routing is specified, specify addresses other than those shown below for the source IPv6 address. • Multicast addresses • Link-local address
The list cannot be applied because 'quantity-oriented' is set for the flow detection mode.	Because `quantity-oriented` is set for the flow detection mode, this access list cannot be applied. To apply `advance access-list` to the interface, set condition-oriented for the flow detection mode.
The list cannot be applied because the prefix length of the IPv6 source address exceeds 64 bits.	Detection conditions where the source IPv6 address of the flow detection conditions is the upper 65 bits or more cannot be applied. The following conditions must be satisfied: • The length of the source IPv6 address of the flow detection conditions must be 64 or less. • `host` is not specified for the source IPv6 address of the flow detection conditions.
The list cannot be applied to the outbound direction of the interface because the list includes a policy-based routing entry.	This access list cannot be applied to the sending side of the interface because the access list includes policy-based routing. Apply access lists that include policy-based routing to the receiving side of the interface. If applying access lists to the sending side of the interface, delete the policy-based routing setting.
The list cannot be applied to this interface because the list includes the 'own-prefix' parameter or the 'own-address' parameter.	This access list includes an `own-prefix` parameter or `own-address` parameter in the flow detection conditions, and so it cannot be applied to the interface. The following conditions must be satisfied to apply an access list including an `own-prefix` parameter or `own-address` parameter to the interface: • An address is set to the interface to be applied. • Only one IPv6 global address is set.

Message	Description
The list name has already been used by another access list.	This access list name has been used for another access list. Specify an access list name that is not being used for another access list or specify the name of an applicable access list.
The number of filter entries exceeds the maximum.	The number of filter entries has exceeded the capacity limit. Use the `show` command to confirm the number of entries used.
The policy-based routing list name cannot be specified.	This policy-based routing list name cannot be specified. Specify a policy-based routing list name that has already been created as the target.
The total number of sequences in access lists and QoS flow lists exceeds the maximum.	The number of sequences for the access lists and QoS flow lists has exceeded the maximum quantity. The number of sequences that can be set is a maximum of 256000 entries for the total combined number of sequences for the access lists and QoS flow lists. You can confirm the number of used sequences by using the `show` command. Use this command to check the number of sequences for the relevant access lists and QoS flow lists. This can be used for the following commands: • `deny (advance access-list)` command • `deny (ip access-list extended)` command • `deny (ip access-list standard)` command • `deny (ipv6 access-list)` command • `deny (mac access-list extended)` command • `permit (advance access-list)` command • `permit (ip access-list extended)` command • `permit (ip access-list standard)` command • `permit (ipv6 access-list)` command • `permit (mac access-list extended)` command • `qos (advance qos-flow-list)` command • `qos (ip qos-flow-list)` command • `qos (ipv6 qos-flow-list)` command • `qos (mac qos-flow-list)` command
There has already been an access list with the same type and direction.	An access list that is the same list type and has the same specified send or receive direction has already been applied. To apply an access list that is the same list type and has the same specified send or receive direction, first, delete the access list that was already applied, and then apply the desired access list.

8.3 Errors when specifying QoS settings

Table 8-2: Error messages displayed when specifying QoS settings

Message	Description
Other qos-queue-group already exists.	Other QoS queue list information is already applied.
The direction of the policer is different from that of the QoS flow list.	The policer entry specified by this QoS flow list and the specified send or receive direction where the QoS flow list is applied do not match. The following conditions must be satisfied: • If a receiving-side policer entry is specified for operation, this is applied to the receiving-side interface. • If a sending-side policer entry is specified for operation, this is applied to the sending-side interface.
The list cannot be applied because 'quantity-oriented' is set for the flow detection mode.	Because `quantity-oriented` is set for the flow detection mode, this list cannot be set. To apply `advance qos-flow-list` to the interface, set `condition-oriented` for the flow detection mode.
The list cannot be applied because the prefix length of the IPv6 source address exceeds 64 bits.	Detection conditions where the source IPv6 address of the flow detection conditions is the upper 65 bits or more cannot be applied. The following conditions must be satisfied: • The length of the source IPv6 address of the flow detection conditions must be 64 or less. • `host` is not specified for the source IPv6 address of the flow detection conditions.
The list cannot be applied to this interface because the list includes the 'own-prefix' parameter or the 'own-address' parameter.	This QoS flow list includes an `own-prefix` parameter or `own-address` parameter in the flow detection conditions, and so it cannot be applied to this interface. The following conditions must be satisfied to apply a QoS flow list including an `own-prefix` parameter or `own-address` parameter to the interface: • An address is set to the interface to be applied. • Only one IPv6 global address is set.
The list name has already been used by another QoS flow list.	This QoS flow list name has been used for another QoS flow list. Specify a QoS flow list name that is not being used for another QoS flow list, or the target QoS flow list name.
The number of QoS flow entries exceeds the maximum.	The number of QoS flow entries has exceeded the capacity limit. The number of sequences that are being used for the QoS flow entries and policer entries can be confirmed using the `show` command.
The policer cannot be deleted because it is still referred to by a QoS flow list.	The specified policer entry is specified in the QoS flow list, and so it cannot be deleted. To delete the policer entry, first delete the specified policer entry from the QoS flow list, and then delete the policer entry.
The policer entry name cannot be specified.	The policer entry name cannot be specified. Specify a policer entry name that has already been created as the target.
The policer entry name has already been used by another policer.	This policer entry name is already used by another policer entry. Either specify a policer entry name that is not being used by another policer entry, or delete the policer entry using the same name.
The port does not support the scheduling mode.	This cannot be set because this is a scheduling mode that is not supported in the target line.
The specified rate value of WFQ is incorrect, or is outside the valid range.	Either the specified WFQ rate is an incorrect value or is outside the setting range.

Message	Description
The total number of sequences in access lists and QoS flow lists exceeds the maximum.	The number of sequences for the access lists and QoS flow lists has exceeded the maximum quantity. The number of sequences that can be set is a maximum of 256000 entries for the total combined number of sequences for the access lists and QoS flow lists. The number of sequences that are being used can be confirmed by using the `show` command. Use this command to check the number of sequences for the relevant access lists and QoS flow lists. This can be used for the following commands: • `deny (advance access-list)` command • `deny (ip access-list extended)` command • `deny (ip access-list standard)` command • `deny (ipv6 access-list)` command • `deny (mac access-list extended)` command • `permit (advance access-list)` command • `permit (ip access-list extended)` command • `permit (ip access-list standard)` command • `permit (ipv6 access-list)` command • `permit (mac access-list extended)` command • `qos (advance qos-flow-list)` command • `qos (ip qos-flow-list)` command • `qos (ipv6 qos-flow-list)` command • `qos (mac qos-flow-list)` command
There has already been a QoS flow list with the same type and direction.	A QoS flow list that is the same list type and has the same specified send or receive direction has already been applied. To apply a QoS flow list that is the same list type and has the same specified send or receive direction, first, delete the QoS flow list that was already applied, and then apply the desired QoS flow list.

8.4 Errors when specifying port mirroring settings

Table 8-3: Error messages displayed when specifying port mirroring settings

Message	Description
A monitor port can be specified only in one monitor session, or in a pair of one tx session and one rx session.	The monitor port can be set only for one monitor session or for one `tx` session and one `rx` session.
The following items conflict: 'the mirror port' and 'the channel group port' cannot be set together.	The mirror port cannot be set for interfaces where a channel group is set.
The following items conflict: 'the mirror port' and 'the IP interface' cannot be set together.	The mirror port cannot be set for interfaces where an IP address is set.
The following items conflict: 'the mirror port' and 'the subinterface' cannot be set together.	The mirror port cannot be set for interfaces where a subinterface is set.
The following items conflict: the mirror port and 'ethernet cfm mep' cannot be set together.	The mirror port cannot be set for interfaces where a MEP used by CFM is set.
The following items conflict: the mirror port and 'lldp enable' cannot be set together.	The mirror port cannot be set for interfaces where the `lldp enable` command is set.
The following items conflict: the mirror port and monitor port. They cannot be set together.	Both mirror port and monitor port settings cannot be specified simultaneously.

8.5 Errors when specifying CFM settings

Table 8-4: Error messages displayed when specifying CFM settings

Message	Description
'ethernet cfm ais enable' cannot be configured for a channel group port.	AIS of an interface participating in a port channel cannot be enabled.
'ethernet cfm enable' cannot be configured for a channel group port.	CFM of an interface participating in a port channel cannot be enabled.
'ethernet cfm lck enable' cannot be configured for a channel group port.	LCK of an interface participating in a port channel cannot be enabled.
MEP cannot be configured for a channel group port.	An MEP cannot be set for an interface that is participating in a port channel.
MEP of the same level cannot be configured to the same interface.	MEP at the same level cannot be set on the same interface.
The Domain name is already configured for a CFM domain. (Domain name=<*name*>)	The specified domain name is already set in the same domain.
	<*name*>: Domain name
The Domain name is already configured for a CFM domain. (MAC address=<*mac*>, ID=<*id*>)	The specified domain name is already set in the same domain.
	<*mac*>: MAC address <*id*>: ID
The following items conflict: 'ethernet cfm mep' and the mirror port cannot be set together.	The MEP used by CFM cannot be set for interfaces that are set to a mirror port.
The MA name is already configured for a CFM domain. (MA name = <*name*>)	The specified MA name is already set in the same domain.
	<*name*>: Indicates the MA name.
The MEG ID is already configured for a MEG Level. (ICC = <*string1*>, UMC = <*string2*>)	The specified MA name is already set in the same domain.
	<*string1*>: ITU carrier code1 <*string2*>: Unique MEG ID code
The MEP ID is already configured for a CFM MEP. (MEP ID = <*mepid*>)	The specified MEP ID has already been set for another MEP.
	<*mepid*>: Indicates the MEP ID.
The number of 'MEP' specifications exceeds the maximum.	The number of MEP settings exceeds the maximum. Delete unnecessary MEP settings.
The VLAN ID is already configured in an MA name. (VLAN ID = <*vlan id*>)	The specified VLAN ID is already being used by another MA name.
	<*vlan id*>: VLAN ID

8.6 Errors when specifying LLDP settings

Table 8-5: Error messages displayed when specifying LLDP settings

Message	Description
The following items conflict: 'lldp enable' and the mirror port cannot be set together.	The `lldp enable` command cannot be set for interfaces that are set to a mirror port.

Index

A

advance access-group 24
advance access-list 26
advance access-list resequence 27
advance qos-flow-group 134
advance qos-flow-list 136
advance qos-flow-list resequence 137

C

cc alarm-priority 224
cc alarm-reset-time 226
cc alarm-start-time 227
cc cos 228
cc enable 229
cc interval 230
command description format 2

D

deny (advance access-list) 29
deny (ip access-list extended) 43
deny (ip access-list standard) 52
deny (ipv6 access-list) 54
deny (mac access-list extended) 62
domain-name 231

E

ethernet cfm ais enable 233
ethernet cfm cc cos 234
ethernet cfm domain-level 236
ethernet cfm enable (global) 237
ethernet cfm enable (interface) 238
ethernet cfm lck enable 239
ethernet cfm mel 240
ethernet cfm mep 241

I

ip access-group [access list] 65
ip access-list extended 67
ip access-list resequence 68
ip access-list standard 70
ip qos-flow-group 139
ip qos-flow-list 141
ip qos-flow-list resequence 142
ipv6 access-list 71
ipv6 access-list resequence 72
ipv6 qos-flow-group 144
ipv6 qos-flow-list 146
ipv6 qos-flow-list resequence 147
ipv6 traffic-filter 74

L

lldp enable 248
lldp hold-count 249
lldp interval-time 250
lldp run 251

M

ma-id 243
mac access-group 76
mac access-list extended 78
mac access-list resequence 79
mac qos-flow-group 149
mac qos-flow-list 151
mac qos-flow-list resequence 152
meg-id 244
monitor session 206

P

permit (advance access-list) 81
permit (ip access-list extended) 96
permit (ip access-list standard) 105
permit (ipv6 access-list) 107
permit (mac access-list extended) 116
policer 154

Q

qos (advance qos-flow-list) 158
qos (ip qos-flow-list) 174
qos (ipv6 qos-flow-list) 184
qos (mac qos-flow-list) 193
qos-queue-group 197
qos-queue-list 199

R

remark [access list] 119
remark [QoS] 202

S

sflow additional-http-port 210
sflow destination 211
sflow extended-information-type 212
sflow forward ingress 214
sflow max-header-size 215
sflow max-packet-size 216
sflow packet-information-type 217
sflow polling-interval 218
sflow sample 219
sflow source 222

T

traffic-shape rate 203