AX6700S/AX6600S/AX6300S Software Manual

Configuration Command Reference Vol. 2

For Version 11.7

AX63S-S010X-30

■ Relevant products

This manual applies to the models in the AX6700S, AX6600S, and AX6300S series of switches. It also describes the functionality of version 11.7 of the software for the AX6700S, AX6600S, and AX6300S series switches. The described functionality is that supported by the OS-S/ OS-SE basic software and optional licenses.

■ 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.

Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and other countries.

IPX is a trademark of Novell, Inc.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and other countries.

Octpower is a registered trademark of NEC Corporation.

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.

VitalQIP and VitalQIP Registration Manager are trademarks of Lucent Technologies.

VLANaccessClient is a trademark of NEC Soft, Ltd.

VLANaccessController and VLANaccessAgent are trademarks of NEC Corporation.

Windows is a registered trademark of Microsoft Corporation 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

January 2012 (Edition 4) AX63S-S010X-30

■ Copyright

History of Amendments

[For version 11.7]

Summary of amendments

Location and title	Changes
4 Access Lists	• The policy-list parameter was added to the following commands: access-list permit (advance access-list) permit (ip access-list extended) • The policy-switch-list parameter was added to the following commands: access-list permit (advance access-list) permit (ip access-list extended) permit (ipv6 access-list) permit (mac access-list extended) • The notes on the following commands were changed: access-list permit (advance access-list) permit (ip access-list extended) permit (ipv6 access-list)
24 SNMP	• The `policy-base` and `informs` parameters were added to the `snmp-server host` command. • The `snmp-server informs` command was added.

In addition to the above changes, minor editorial corrections were made.

[For version 11.5]

Summary of amendments

Item	Changes
SNMP	• The `static-route` parameter was added to the `snmp-server host` command.

[For version 11.4]

Summary of amendments

Item	Changes
Layer 2 Authentication	• This chapter was added.
Web Authentication	• The `fqdn` parameter was added to the `web-authenticaion ip address` command. • The following commands were added: web-authentication redirect-mode web-authentication redirect-vlan
MAC-based Authentication	• The following commands were added: mac-authentication auto-logout mac-authentication dynamic-vlan max-user
DHCP Snooping	• This chapter was added.
Redundancy Control for NIFs	• This chapter was added.
Error Messages Displayed When Editing the Configuration	• The subsection *DHCP snooping information* was added.

[For version 11.3]

The chapter Flow Mode and all subsequent chapters that were in the manual Configuration Command Reference Vol. 1 up to version 11.2 were moved to this manual.

For details about the summary of amendments for version 11.2 and earlier, see *Configuration Command Reference Vol. 1 For Version 11.7*.

Summary of amendments

Item	Changes
Access Lists	• A parameter that specifies an operation of access list logging was added to the following commands: access-list deny (advance access-list) deny (ip access-list extended) deny (ip access-list standard) deny (ipv6 access-list) deny (mac access-list extended)
Access List Logging	• This chapter was added.
Log Data Output Functionality	• A description of access list logging was added to the following commands: logging email-event-kind logging event-kind

Preface

Applicable products and software versions

This manual applies to the models in the AX6700S, AX6600S, and AX6300S series of switches. It also describes the functionality of version 11.7 of the software for the AX6700S, AX6600S, and AX6300S series switches. The described functionality is that supported by the OS-S/OS-SE basic software and optional licenses.

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.

Unless otherwise noted, this manual describes functionality applicable to AX6700S, AX6600S, and AX6300S series switches. Functionality specific to a model is indicated as follows:

[AX6700S]:

The description applies to the AX6700S series.

[AX6600S]:

The description applies to the AX6600S series.

[AX6300S]:

The description applies to the AX6300S series.

Unless otherwise noted, this manual describes functionality applicable to the basic software OS-S/OS-SE. Functionality specific to an optional license is indicated as follows:

[OP-BGP]:

The description applies to the OP-BGP optional license.

[OP-DH6R]:

The description applies to the OP-DH6R optional license.

[OP-MBSE]:

The description applies to the OP-MBSE optional license.

[OP-NPAR]:

The description applies to the OP-NPAR optional license.

[OP-VAA]:

The description applies to the OP-VAA optional license.

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 Switch.

Readers must have an understanding of the following:

- The basics of network system management

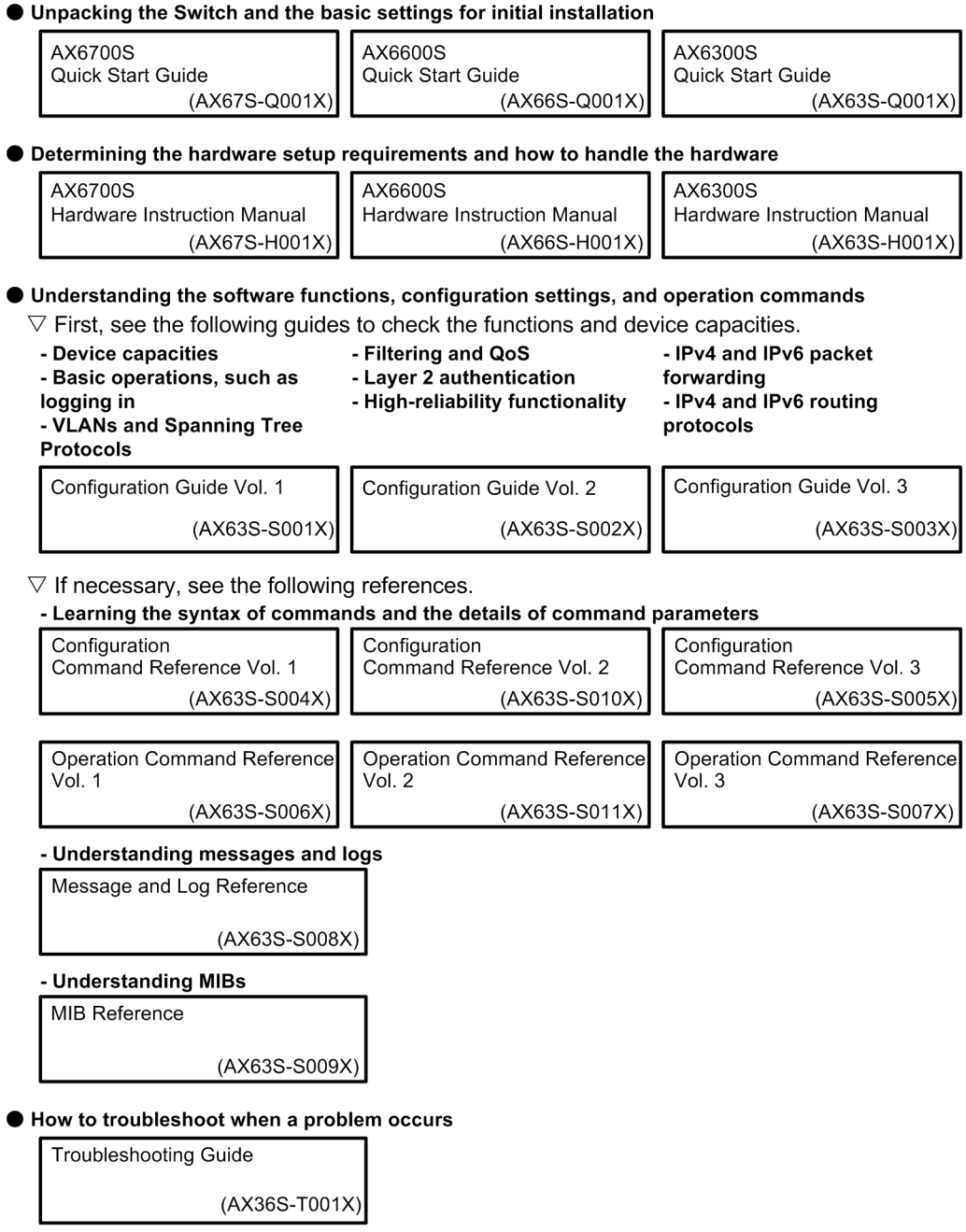
Manual URL

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 Switch.



Conventions: The terms "Switch" and "switch"

The term Switch (upper-case "S") is an abbreviation for any or all of the following models:

AX6700S series switch

AX6600S series switch

AX6300S series switch

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

Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit
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)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic Switching Unit
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
CSU	Control and Switching Unit
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
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
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LLRLQ	Low Latency Rate Limited Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MSU	Management and Switching Unit
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NIF	Network Interface
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PRI	Primary Rate Interface

PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PSP	Packet Switching Processor
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
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
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

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

PART 5: Layer 2 Authentication

8. Layer 2 Authentication 301

9. IEEE802.1X 305

PART 6: Security

PART 7: High Reliability Based on Redundant Configurations

PART 10: Management of Neighboring Device Information

PART 11: Port Mirroring

PART 12: Configuration Error Messages

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 changes to values for configuration information in memory are immediately effective, or whether they take effect only after temporarily stopping operation, such as by restarting the switch.

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

#	Prompt displayed for the command mode	Description	Command for mode transition
1	(config)	Global configuration mode	# enable # configure
2	(config-line)	Configures remote login and console.	(config)# line vty (config)# line console
3	(config-if)	Configures an interface.	(config)# interface
4	(config-if-range)	Configures multiple interfaces.	(config)# interface range
5	(config-vlan)	Configures VLAN.	(config)# vlan
6	(config-mst)	Configures Multiple Spanning Tree	(config)# spanning-tree mst configuration
7	(config-axrp)	Configures the Ring Protocol.	(config)# axrp
8	(config-gsrp)	Configures GSRP.	(config)# gsrp
9	(config-adv-acl)	Configures an Advance filter.	(config)# advance access-list
10	(config-ext-nacl)	Configures an IPv4 packet filter.	(config)# ip access-list extended
11	(config-std-nacl)	Configures an IPv4 address filter.	(config)# ip access-list standard
12	(config-ipv6-acl)	Configures an IPv6 filter.	(config)# ipv6 access-list
13	(config-ext-macl)	Configures a MAC filter.	(config)# mac access-list extended
14	(config-adv-qos)	Configures Advance QoS.	(config)# advance qos-flow-list
15	(config-ip-qos)	Configures IPv4 QoS.	(config)# ip qos-flow-list
16	(config-ipv6-qos)	Configures IPv6 QoS.	(config)# ipv6 qos-flow-list
17	(config-mac-qos)	Configures MAC QoS.	(config)# mac qos-flow-list
18	(dhcp-config)	Configures DHCP	(config)# ip dhcp pool
19	(config-dhcp)	Configures IPv6 DHCP (PD).	(config)# ipv6 dhcp pool
20	(config-route-map)	Configures a route map.	(config)# route-map
21	(config-rtr-rip)	Configures RIPng.	(config)# ipv6 router rip
22	(config-router)	Configures RIP.	(config)# router rip
		Configures OSPF.	(config)# router ospf
		Configures BGP4/BGP4+.	(config)# router bgp
23	(config-rtr)	Configures OSPFv3.	(config)# ipv6 router ospf
24	(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

#	Prompt displayed for the command mode	Description	Command for mode transition
		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
25	(config-auto-cf)	Configures auto-config.	(config)# auto-config
26	(config-netconf)	Configures netconf.	(config)# netconf.
27	(config-view)	Configures view.	(config)# parser view
28	(config-sh-nif)	Configures shaper mode.	(config)# shaper nif
29	(config-vrf)	Configures config-vrf.	(config)# vrf definition
30	(config-ether-cfm)	Configures the domain name and MA.	(config)# ethernet cfm domain
31	(config-track-object)	Configures the policy-based routing tracking functionality.	(config)# track-object
32	(config-pol)	Configures policy-based routing list information.	(config)# policy-list
33	(config-pol-sw)	Configures policy-based switching list information.	(config)# policy-switch-list

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.	ip access-list standard inbound1
Host name	For a 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
IPv4 address, IPv4 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 (:).	3ffe:501:811:ff03::87ff:fed0:c7e0
Specification of multiple interfaces	Set the information about multiple interfaces. Specifiable interfaces are gigabitethernet, tengigabitethernet, vlan, and port-channel. You can specify gigabitethernet and tengigabitethernet at the same time, but cannot specify any other interfaces at the same time. The following are the input formats: • For gigabitethernet interface range gigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>] • For tengigabitethernet interface range tengigabitethernet <*nif no.*>/<*port no.*> [- <*port no.*>] • For vlan interface range vlan <*vlan id*> [- <*vlan id*>] • For port-channel interface range port-channel <*channel group number*> [- <*channel group number*>] You can specify no more than 16 of the above input formats, separating each by a comma (,).	interface range gigabitethernet 1/1-3 interface range gigabitethernet 1/1-3, tengigabitethernet 3/1 interface range vlan 1-100
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.	switchport trunk allowed vlan add 100200-210 switchport trunk allowed vlan remove 100200-210

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
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"

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

The following tables list the range of parameter <*nif no.*> and <*port no.*> values.

Table 1-5: Range of <nif no.> values

#	Model	Range of <nif no.> values
1	AX6708S	1 to 8
2	AX6604S	1 to 4
3	AX6608S	1 to 8
4	AX6304S	1 to 4
5	AX6308S	1 to 8

Table 1-6: Range of <port no.> values [AX6700S] [AX6600S]

#	NIF type name abbreviation	Range of <port no.> values
1	NK1G-24T	1 to 24
2	NK1G-24S	1 to 24
3	NK1GS-8M	1 to 8
4	NK10G-4RX	1 to 4
5	NK10G-8RX	1 to 8

Table 1-7: Range of <port no.> values [AX6300S]

#	NIF type name abbreviation	Range of <port no.> values
1	NH1G-16S	1 to 16
2	NH1G-24T	1 to 24
3	NH1G-24S	1 to 24
4	NH1G-48T	1 to 48
5	NH1GS-6M	1 to 6
6	NH10G-1RX	1
7	NH10G-4RX	1 to 4
8	NH10G-8RX	1 to 8

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

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

Table 1-8: Range of <channel group number> values

#	Model	Range of values
1	AX6304S/AX6604S	1 to 48
2	AX6308S/AX6608S/AX6708S	1 to 63

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

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

Table 1-9: Range of <vlan id> values

#	Range of values
1	1 to 4095

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

If *<vlan id list>* is written in the parameter input format, use a hyphen (-) or comma (,) to set multiple VLAN IDs. You can also set one VLAN ID, as when *<vlan id>* is written as the parameter input format. The range of values that can be set is the same as the range of *<vlan id>* values above. If there are large amounts of information set for *<vlan id list>*, the configuration information might be displayed over multiple lines. Conversely, if the information set in *<vlan id list>* is reduced by edits made to VLANs using `add/remove`, multiple lines of configuration information might be consolidated into one line.

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

1-3,5,10

Example of a specification displayed in multiple lines:

switchport trunk allowed vlan 100200300...

switchport trunk allowed vlan add 400500...

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

If *<interface id list>* is written in parameter input format, use a hyphen (-) or commas (,) as delimiters to specify multiple interfaces of the type gigabitethernet or tengigabitethernet. You can also specify just one interface of the type gigabitethernet or tengigabitethernet. The following are the input formats for gigabitethernet and tengigabitethernet interfaces:

- For gigabitethernet

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

- For tengigabitethernet

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

The ranges of specifiable values for *<nif no.>* and *<port no.>* in *<nif no.>*/*<port no.>* `[-` *<port no.>*`]` are the same as the ranges of *<nif no.>* and *<port no.>* values in the above tables.

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>* [OP-NPAR]

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

Table 1-10: Range of <vrf id> values

#	VRF operation mode	Range of values
1	Not specified	Not configurable
2	axrp-enable axrp-enable-ipv4-ipv6	2 to 64
3	l2protocol-disable l2protocol-disable-ipv4-ipv6	2 to 250
4	gsrp-enable-ipv4-ipv6	2 to 125

Chapter 2. Flow Mode

flow mac mode

flow mac mode

Configures MAC mode for the filtering and QoS functionality on a VLAN interface. This command enables flow detection for IP packets forwarded on Layer 2, based on the MAC access list and MAC QoS flow list.

This command is used to set basic operating conditions for the hardware. Before you use this command to change conditions, if any of the following command settings are set you must delete them on the applicable VLAN interface.

- ip access-group
- ipv6 traffic-filter
- mac access-group
- ip qos-flow-group
- ipv6 qos-flow-group
- mac qos-flow-group

Accordingly, you must set this command during the first step of actual operation. We recommend that you do not make any changes during operation.

If you do not set this command or if you have deleted information, operation proceeds as described in *Default behavior*.

Syntax

To set information:

flow mac mode

To delete information:

no flow mac mode

Input mode

`(config-if)`

Parameters

None

Default behavior

The MAC access list and MAC QoS flow list perform flow detection only for non-IP packets.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set if the flow distribution pattern is `defaut standard`, `default extended`, `filter-only extended`, `qos-only extended`, `filter extended`, or `qos extended`.

Related commands

ip access-group

ipv6 traffic-filter

mac access-group

ip qos-flow-group

ipv6 qos-flow-group

mac qos-flow-group

Chapter

3. VLAN List

vlan-list

vlan-list

Creates a VLAN list to be used in the access list and QoS flow list.

No more than 1024 VLAN lists can be created for a device.

Syntax

To set or change information:

vlan-list <*vlan id list name*> <*vlan id list*>

To delete information:

no vlan-list <*vlan id list name*>

Input mode

`(config)`

Parameters

<*vlan id list name*>

Specifies the VLAN list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string of no more than 31 characters with an alphabetic character for the first character.

   For details, see *Any character string* in *Specifiable values for parameters*. You cannot specify a space.

<*vlan id list*>

Specifies multiple VLAN IDs at one time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable 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. You cannot delete a VLAN list if it is specified in a flow detection condition in an access list or QoS flow list. Delete the VLAN list from the access list or QoS flow list before executing this command.

Related commands

access-list

deny (advance access-list)

deny (ip access-list extended)

deny (ipv6 access-list)

deny (mac access-list extended)

permit (advance access-list)

permit (ip access-list extended)

permit (ipv6 access-list)

permit (mac access-list extended)

qos (advance qos-flow-list)

qos (ip qos-flow-list)

qos (ipv6 qos-flow-list)

qos (mac qos-flow-list)

Chapter 4. Access Lists

Names and values that can be specified
access-list
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

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 4-1: 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 4-2: 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 4-3: 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 4-4: 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 4-5: 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 name

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

Table 4-6: 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 name

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

Table 4-7: 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 name

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

Table 4-8: 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 name

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

Table 4-9: Ethernet type names that can be specified

Ethernet type name	Ethernet value	Remarks
appletalk	0x809b	
arp	0x0806	
axp	0x88f3	Alaxala Protocol
eapol	0x888e	
gsrp	--#	Filters 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 4-10: Destination MAC address names that can be specified

Destination address specification	Destination address	Destination address mask
bpdu	0180.C200.0000	0000.0000.0000
cdp	0100.0CCC.CCCC	0000.0000.0000
lacp	0180.C200.0002	0000.0000.0000
lldp	0100.8758.1310	0000.0000.0000
oadp	0100.4C79.FD1B	0000.0000.0000
pvst-plus-bpdu	0100.0CCC.CCCD	0000.0000.0000

Destination address specification	Destination address	Destination address mask
slow-protocol	0180.C200.0002	0000.0000.0000

Message name (ICMP)

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

Table 4-11: 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
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4

Message name	Message	Type	Code
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 4-12: 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
packet-too-big	Packet too big	2	Not specified

Message name	Message	Type	Code
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

Number of access lists that can be created

The number of access lists that can be created is the number of names that can be used as access list IDs. The maximum number of lists that can be created is shown below (in the total for <*access list name*> and <*access list number*> of the corresponding configuration). Note that if you specify only <*access list number*>, a maximum of 1599 lists can be created.

- For AX6700S series switches:

  The following table lists the number of access lists that can be created for each BSU type.

  Table 4-13: Number of access lists that can be created for each BSU type

BSU type	Access lists	Filter conditions
All models	8574 lists	32000 entries#

  #: Flow detection and action specification entries in the QoS flow list are included.

- For AX6600S series switches:

  The number of access lists and filter conditions that can be created for a Switch depends on the CSU type. The following table lists the number of access lists that can be created for each CSU type.

  Table 4-14: Number of access lists that can be created for each CSU type

CSU type	Access lists	Filter conditions
CSU-1A	2000 lists	4000 entries
CSU-1B	8574 lists	32000 entries#

  #: Flow detection and action specification entries in the QoS flow list are included.

- For AX6300S series switches:

  The number of access lists and filter conditions that can be created for a Switch depends on the MSU type. The following table lists the number of access lists that can be created for each MSU

type.

Table 4-15: Number of access lists that can be created for each MSU type

MSU type	Access lists	Filter conditions
MSU-1A and MSU-1A1	2000 lists	4000 entries
MSU-1B and MSU-1B1	8574 lists	32000 entries#

#: Flow detection and action specification entries in the QoS flow list are included.

Number of specifications that can be set for an interface

The number of specifications that can be set for an interface is the total number of access lists that can be set for an interface. The maximum number of lists that can be created is shown below.

Specifications are counted separately for the receiving side, sending side, and the forwarding type. 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. Similarly, if both Layer 2 forwarding and Layer 3 forwarding are set for the same interface, it is counted as two lists.

- For AX6700S series switches:

  The following table lists the number of specifications that can be set for an interface for each BSU type.

  Table 4-16: Number of specifications that can be set for an interface for each BSU type

BSU type	Number of specifications that can be set
All models	8574 lists

- For AX6600S series switches:

  The number of `ip access-group`, `ipv6 traffic-filter`, `mac access-group`, and `advance access-group` settings available for a Switch depends on the CSU type. The following table lists the number of specifications that can be set for an interface for each CSU type.

  Table 4-17: Number of specifications that can be set for an interface for each CSU type

CSU type	Number of specifications that can be set
CSU-1A	2000 lists
CSU-1B	8574 lists

- For AX6300S series switches:

  The number of `ip access-group`, `ipv6 traffic-filter`, `mac access-group`, and `advance access-group` settings available for a Switch depends on the MSU type. The following table lists the number of specifications that can be set for an interface for each MSU type.

  Table 4-18: Number of specifications that can be set for an interface for each MSU type

MSU type	Number of specifications that can be set
MSU-1A and MSU-1A1	2000 lists
MSU-1B and MSU-1B1	8574 lists

Examples for calculating the number of access lists that can be created and the number of specifications that can be set for an interface

The following table provides examples for calculating the number of access lists that can be created and the number of specifications that can be set for an interface.

Table 4-19: Examples for calculating the number of access lists that can be created and the number of specifications that can be set for an interface

Sample code	Number of access lists to be created	Number of specifications set for the interface

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 layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 list	1 list

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 layer2-forwarding`
 	
`interface gigabitethernet 1/2`
`ip access-group AAA in layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 list	2 lists

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 layer2-forwarding`
`ip access-group AAA out layer2-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 list	2 lists

In this example, access list `AAA` is created and `layer2-forwarding` and `layer3-forwarding` is set for `inbound` on the VLAN 2 interface.
`interface vlan 2`
`ip access-group AAA in layer2-forwarding`
`ip access-group AAA in layer3-forwarding`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 list	2 lists

Sample code	Number of access lists to be created	Number of specifications set for the interface

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 layer2-forwarding`
 	
`interface gigabitethernet 1/2`
`ip access-group BBB in layer2-forwarding`
 	
`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

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 layer2-forwarding`
`ip access-group BBB out layer2-forwarding`
 	
`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

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 lists

access-list

Configures an access list to serve 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. An IPv4 address filter filters packets based on IPv4 address. An IPv4 packet filter filters based on source IPv4 address, destination IPv4 address, VLAN ID, user priority, fragmented packet, ToS field value, port number, TCP flag, ICMP type, ICMP code, and IGMP type.

Note that syntax is different if you specify fragmented packets as the detection condition. See *When "packet is fragmented" is a condition* of *Syntax*.

You can use one access list ID and specify multiple filter conditions.

For details of the number of access lists and filter conditions that can be created for a Switch, see *Number of access lists that can be created*.

If you specify `permit` for the filter action, you can specify parameters for policy-based routing. In this case, if you use access group commands to apply the target access list to an interface, specify the inbound side of the VLAN interface, and Layer 3 forwarding as the forwarding type.

If you specify `permit` for the filter action, you can specify parameters for policy-based switching. If you use access group commands to apply the target access list to an interface, specify the inbound side of the Ethernet interface.

Syntax

To set or change information:

Configuring supplementary information

access-list <*access list number*> remark <*remark*>

Configures an IPv4 address filter.

access-list <*access list number*> [<*sequence*>] permit {<*ipv4*> [<*ipv4 wildcard*>] | host <*ipv4*> | any}

access-list <*access list number*> [<*sequence*>] deny {<*ipv4*> [<*ipv4 wildcard*>] | host <*ipv4*> | any} [<*action-specification*>]

Action specification

action log

Configures an IPv4 packet filter.

access-list <*access list number*> [<*sequence*>] permit {<*filter-condition*>} [<*action-specification*>]

access-list <*access list number*> [<*sequence*>] deny {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

- When the upper-layer protocol is other than TCP, UDP, ICMP, and IGMP

  {deny | permit} {ip | <*protocol*>} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is TCP

{deny | permit} tcp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is UDP

  {deny | permit} udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is ICMP

  {deny | permit} icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is IGMP

  {deny | permit} igmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [<*igmp type*>][{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When "packet is fragmented" is a condition

  {deny | permit} {ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [fragments] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

Action specification

- For `permit {`<*filter-condition*>`}`:

  action {policy interface vlan <*vlan id*> next-hop <*next hop ipv4*> | policy-list <*policy list no.*> | policy-switch-list <*policy switch list no.*>}

- For `deny {`<*filter-condition*>`}`:

  action log

To delete information:

no access-list <*access list number*>

Input mode

(config)

Parameters

<*access list number*>

Specifies the identifier used to identify the access list.

This identifier is used to reference the access list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 199, or 1300 to 2699 (in decimal).

   Identifiers in the range from 1 to 99 and from 1300 to 1999 (in decimal) are dedicated to IPv4 address filtering.

   Identifiers in the range from 100 to 199 and from 2000 to 2699 are dedicated to IPv4 packet filtering.

remark <*remark*>

Sets supplementary information for an access list.

One line can be set for one ID. Entering new information overwrites the existing information.

1. Default value when this parameter is omitted:

   The initial value is null.

2. Range of values:

   Enclose a character string of no more than 64 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*.

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

- Filter condition parameters

{deny | permit}

Specifies the filter action to take when filter conditions are met.

Specifying `deny` denies access.

Specifying `permit` permits access.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `deny` or `permit`.

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

Specifies the IPv4 address.

To specify all IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*ipv4*> `[`<*ipv4 wildcard*>`]`, `host` <*ipv4*>, or `any`.

   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*>.

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

   If `any` is specified, IPv4 addresses are not used as a filter condition.

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

{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 4-1: Protocol names that can be specified (IPv4)*.

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

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv4*> <*source ipv4 wildcard*>, `host` <*source ipv4*>, `any`, `own-address` <*source ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*source ipv4 start*> <*source ipv4 end*>.

   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.

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

If `any` is specified, the source IPv4 address is not used as a filter condition.

`own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

`range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

If `own-address` is specified, the filter condition is the source IPv4 address that has been set on the target interface.

If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

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.

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 4-3: Port names that can be specified for TCP* and *Table 4-4: Port names that can be specified for UDP (IPv4)*.

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

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

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

   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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv4*> <*destination ipv4 wildcard*>, `host` <*destination ipv4*>,

`any`, `own-address` <*destination ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*destination ipv4 start*> <*destination ipv4 end*>.

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.

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

If `any` is specified, the destination IPv4 address is not used as a filter condition.

`own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

`range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

If `own-address` is specified, the filter condition is the destination IPv4 address that has been set on the target interface.

If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

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.

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 4-3: Port names that can be specified for TCP* and *Table 4-4: Port names that can be specified for UDP (IPv4)*.

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

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

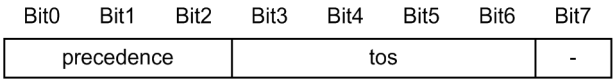
   If `range` is specified, the filter condition is in the range from <*destination port start*> to <*destination port end*>.

   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:

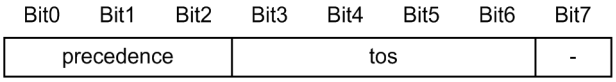
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 4-6: 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:

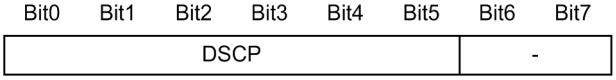
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 4-7: 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 4-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 4-11: 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 when 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.

Fragments

Specifies the second and subsequent fragmented packets.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

policy interface vlan <*vlan id*> next-hop <*next hop ipv4*>

Specifies the output destination for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   <*vlan id*>

   For details about the VLAN ID, see *Specifiable values for parameters*.

   <*next hop ipv4*>

   Specifies a next-hop IPv4 address.

   Specify an address in the network that connects to the specified destination interface. However, you cannot specify the direct broadcast address of the network connected to the specified destination interface or an address that has been set on the specified destination interface.

policy-list <*policy list no.*>

Specifies the list number for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   Specify the list number for policy-based routing that was set by using the `policy-list` command.

policy-switch-list <*policy switch list no.*>

Specifies the list number for policy-based switching.

1. Default value when this parameter is omitted:

   None. (Policy-based switching is not used.)

2. Range of values:

   Specify the list number for policy-based switching that was set by using the `policy-switch-list` command.

log

The packets discarded by the specified access list are included in access list logging.

1. Default value when this parameter is omitted:

   None. (Access list logging is not used.)

2. Range of values:

   None

Default behavior

None

Impact on communication

If an entry is added or 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. In IPv4 address filtering, if you omit the address mask when specifying the target IP host address, 0.0.0.0 is used as the mask.
2. For <*access list number*>, you can use 1 to 99 or 1300 to 1999 in the `ip access-list`

`standard` command.

3. For <*access list number*>, you can use 100 to 199 or 2000 to 2699 in the `ip access-list extended` command.
4. When `255.255.255.255` is entered for an IPv4 address wildcard mask, a source address wildcard mask, or a destination address wildcard mask, `any` is displayed.
5. If *nnn*. *nnn*. *nnn*. *nnn* `0.0.0.0` is entered as the IPv4 address, the source address, and the destination address, `host` *nnn*. *nnn*. *nnn*. *nnn* is displayed.
6. If policy-based routing is specified for the action parameter, the following addresses cannot be specified for the source IPv4 address and destination IPv4 address that are set for filtering conditions:

   Source IPv4 address

   Multicast address and internal loopback address

   Destination IPv4 address

   Multicast address, restricted broadcast address, and internal loopback address
7. If policy-based switching is specified for the action parameter, specify the VLAN ID set in the specified policy-based switching list for `vlan` of the filter condition parameters. Note that you cannot specify a VLAN list name at this time.
8. Before specifying `log` as an action in an access list, enable logging by using the `system hardware-mode` command with the `access-log` parameter.

Related commands

ip access-group

ip access-list resequence

vlan-list

policy-list

policy-switch-list

advance access-group

Applies an Advance access list to an Ethernet interface or a VLAN interface, and enables the Advance filtering functionality.

For details of the number of specifications that can be set for an interface per device, see *Number of specifications that can be set for an interface*.

If you apply an access list with the policy-based routing parameter specified, specify the inbound side of the VLAN interface.

If you apply an access list with the policy-based switching parameter specified, specify the inbound side of the Ethernet interface.

Syntax

To set information:

- Ethernet interface

  advance access-group <*access list name*> {in | out} layer2-forwarding
- VLAN interface

  advance access-group <*access list name*> {in | out} layer2-and-layer3-forwarding

To delete information:

- Ethernet interface

  no advance access-group <*access list name*> {in | out} layer2-forwarding
- VLAN interface

  no advance access-group <*access list name*> {in | out} layer2-and-layer3-forwarding

Input mode

`(config-if)`

Parameters

<*access list name*>

Specifies the identifier of the Advance filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.
2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

layer2-and-layer3-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-and-layer3-forwarding` detects packets forwarded on Layer 2 and Layer 3 in flow detection.

This parameter has an effect only when it is applied to a VLAN interface.

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 applied to an interface, IP packets received at the interface are 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. On an Ethernet interface, you can set one Advance filter for each of Inbound and Outbound.

   If a filter has already been set, first remove it and then set it again.

2. If you specify a non-existent Advance filter, this will be ignored. The identifier of the Advance filter is registered.

3. You can set an Advance access list if the flow distribution pattern is `default standard-advance`, `default extended-advance`, `filter-only extended-advance`, `filter extended-advance`, or `qos extended-advance`.

4. When `mac-ip` is specified for the flow detection condition type and the `own-address` or `own` parameter is specified in the flow detection condition, you can set an Advance access list if an IPv4 address is set for the target interface.

5. When `mac-ipv6` is specified for the flow detection condition type and the `own-address` or `own` parameter is specified in the flow detection condition, you can set an Advance access list if one IPv6 global address only is set for the target interface.

6. When an Advance access list is to be applied to an Ethernet interface and a VLAN parameter is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.

7. When an Advance access list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.
8. If the distribution pattern of path-related table entries is `ipv4-uni standard` or `ipv4-uni extended`, you cannot set an IPv6 filter with IPv6 policy-based routing specified. You can set it if the distribution pattern of path-related table entries is other than above.
9. Before specifying `log` as an action in an access list, enable logging by using the `system hardware-mode` command with the `access-log` parameter.

Related commands

advance access-list

advance access-list

Configures an access list to serve as an Advance filter.

You can use one access list ID and specify multiple filter conditions.

For details of the number of access lists and filter conditions that can be created for a Switch, see *Number of access lists that can be created*.

If you specify `permit` for the filter action, you can specify parameters for policy-based routing. If you use access group commands to apply the target access list to an interface, specify the inbound side of the VLAN interface.

If you specify `permit` for the filter action, you can specify parameters for policy-based switching. If you use access group commands to apply the target access list to an interface, specify the inbound (reception) side of an Ethernet interface.

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 identifier of the Advance filter that is to be set.

The Switch enters `config-adv-acl` mode.

Names that have already been used for IPv4 address filters, IPv4 packet filters, and MAC filters cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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 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 filter 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 the identifier of the Advance filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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 extended

deny (advance access-list)

Specifies the conditions by which the Advance filter denies access.

Syntax

To set or change information:

[<*sequence*>] deny mac {<*filter-condition*>} [<*action-specification*>]

[<*sequence*>] deny mac-ip {<*filter-condition*>} [<*action-specification*>]

[<*sequence*>] deny mac-ipv6 {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

For `mac` {<*filter-condition*>}:

This filter 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} [<*ethernet type*>][vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

For `mac-ip` {<*filter-condition*>}:

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

- When "packet is not fragmented" is a condition, and the upper-layer protocol is 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ip | <*protocol*>} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} tcp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} igmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [<*igmp type*>] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is fragmented" is a condition

  mac-ip {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [fragments] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

For `mac-ipv6 {`<*filter-condition*>`}`:

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

- When the upper-layer protocol is 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ipv6 | <*protocol*>} {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*source ipv6 start*> <*source ipv6 end*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} tcp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | 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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} udp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} icmp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*source ipv6 start*> <*source ipv6 end*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority

<*priority*>] [ctag-vlan <*vlan id*>]}]

Action specification

action log

To delete information:

no <*sequence*>

Input mode

`(config-adv-acl)`

Parameters

<*sequence*>

Sets the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the source MAC address.

To specify all source MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source mac*> <*source mac mask*>, `host` <*source mac*>, or `any`.

   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.

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

   If `any` is specified, the source MAC address is not used as a filter condition.

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

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol}

Specifies the destination MAC address.

To specify all destination MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Specify <*destination mac*> <*destination mac mask*>, host <*destination mac*>, any, bpdu, cdp, lacp, lldp, oadp, pvst-plus-bpdu, or slow-protocol.

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.

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

If `any` is specified, the destination MAC address is not used as a filter condition.

If `bpdu` is specified, BPDU control packets are used as the filter condition.

If `cdp` is specified, CDP control packets are used as the filter condition.

If `lacp` or `slow-protocol` is specified, slow protocol packets are used as the filter condition.

This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD functionality.

If `lacp` is specified, LACP control packets are used as the filter condition.

If `lldp` is specified, LLDP control packets are used as the filter condition.

If `oadp` is specified, OADP control packets are used as the filter condition.

If `pvst-plus-bpdu` is specified, PVST+ control packets are used as the filter condition.

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 4-9: Ethernet type names that can be specified*.

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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.

ctag-untagged

Specifies detection of packets with no customer tag.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

ctag-user-priority <*priority*>

Specifies a user priority for the customer 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.

ctag-vlan <*vlan id*>

Specifies a VLAN ID for the customer 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 4-1: 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 4-2: Protocol*

names that can be specified (IPv6).

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

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv4*> <*source ipv4 wildcard*>, `host` <*source ipv4*>, `any`, `own-address` <*source ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*source ipv4 start*> <*source ipv4 end*>.

   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.

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

   If `any` is specified, the source IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the source IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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 | range-address <*source ipv6 start*> <*source ipv6 end*>}

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv6*>`/`<*length*>, `own-address` <*own address length*>, `host` <*source ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*source ipv6 start*> <*source ipv6 end*>.

   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.

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

If `any` is specified, the source IPv6 address is not used as a filter condition.

`own-address` and `own` are valid only for the `traffic-filter` command for a VLAN interface.

`range-address` is valid only for the `traffic-filter` command for an Ethernet interface or a VLAN interface.

If `own-address` is specified, the filter condition is the source IPv6 address that has been set as the IPv6 global address on the target interface.

If `own` is specified, the filter conditions are the source IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

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.

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 4-3: Port names that can be specified for TCP*, *Table 4-4: Port names that can be specified for UDP (IPv4)*, and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

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

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

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

   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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv4*> <*destination ipv4 wildcard*>, `host` <*destination ipv4*>, `any`, `own-address` <*destination ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*destination ipv4 start*> <*destination ipv4 end*>.

   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.

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

   If `any` is specified, the destination IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the destination IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv6*>/<*length*>, `own-address` <*own address length*>, `host` <*destination ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*destination ipv6 start*> <*destination ipv6 end*>.

   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 `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

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

If `any` is specified, the destination IPv6 address is not used as a filter condition.

`own-address` and `own` are valid only for the `traffic-filter` command for a VLAN interface.

`range-address` is valid only for the `traffic-filter` command for an Ethernet interface or a VLAN interface.

If `own-address` is specified, the filter condition is the destination IPv6 address that has been set as the IPv6 global address on the target interface.

If `own` is specified, the filter conditions are the destination IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

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.

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 4-3: Port names that can be specified for TCP*, *Table 4-4: Port names that can be specified for UDP (IPv4)*, and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

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

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

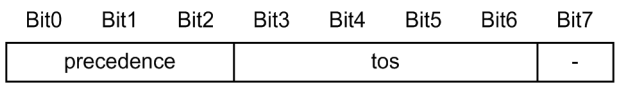
   If `range` is specified, the filter condition is in the range from <*destination port start*> to <*destination port end*>.

   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:

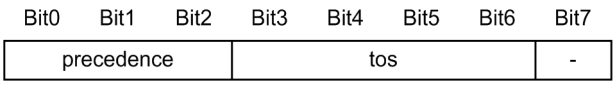
Specify 0 to 15 (in decimal) or a tos name.

For details about the tos names that can be specified, see *Table 4-6: 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 4-7: 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:

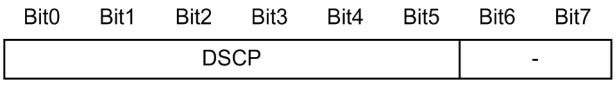
   Specify 0 to 255 in decimal.

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.

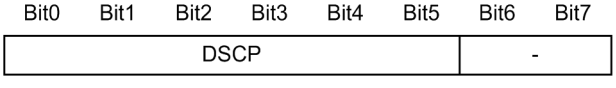
Its value is compared with the first 6 bits in the ToS field of the received packet.



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 six 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 4-8: DSCP names*

that can be specified.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst`

to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 4-11: Message names that can be specified for ICMP (IPv4)* and *Table 4-12: 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 when 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.

Fragments

Specifies the second and subsequent fragmented packets.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

- Action parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

log

The packets discarded by the specified access list are included in access list logging.

1. Default value when this parameter is omitted:

   None. (Access list logging is not used.)

2. Range of values:

   None

Default behavior

None

Impact on communication

If an entry is added or 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 a protocol name is set for the destination MAC address, or if the address of a protocol name that can be set is set, the protocol name is displayed. For details about the address of a protocol name that can be specified as the destination MAC address, *Table 4-10: Destination MAC address names that can be specified*.

   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. When `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 *nnn*.*nnn*.*nnn*.*nnn* `0.0.0.0` is entered as the source IPv4 address and the destination IPv4 address, `host` *nnn*.*nnn*.*nnn*.*nnn* is displayed.
5. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/0` is entered as the source IPv6 address and the destination IPv6 address, `any` is displayed.
6. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/128` is entered as the source IPv6 address and the destination IPv6 address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn* is displayed.

Related commands

advance access-group

advance access-list resequence

permit (advance access-list)

remark

vlan-list

deny (ip access-list extended)

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

Note that syntax is different if you specify fragmented packets as the detection condition. See *When "packet is fragmented" is a condition* of *Syntax*.

Syntax

To set or change information:

[<*sequence*>] deny {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

- When the upper-layer protocol is other than TCP, UDP, ICMP, and IGMP

  {ip | <*protocol*>} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is TCP

  tcp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] |[{ack|+ack|-ack}] [{fin|+fin|-fin}] [{psh|+psh|-psh}] [{rst|+rst|-rst}] [{syn|+syn|-syn}] [{urg|+urg|-urg}]}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is UDP

  udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is ICMP

  icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is IGMP

igmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [<*igmp type*>] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When "packet is fragmented" is a condition

  {ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [fragments] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

Action specification

action log

To delete information:

no <*sequence*>

Input mode

`(config-ext-nacl)`

Parameters

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{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 4-1: Protocol names that can be specified (IPv4)*.

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

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv4*> <*source ipv4 wildcard*>, `host` <*source ipv4*>, `any`, `own-address` <*source ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*source ipv4 start*> <*source ipv4 end*>.

   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.

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

   If `any` is specified, the source IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the source IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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.

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 4-3: Port names that can be specified for TCP* and *Table 4-4: Port names that can be specified for UDP (IPv4)*.

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

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

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

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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv4*> <*destination ipv4 wildcard*>, `host` <*destination ipv4*>, `any`, `own-address` <*destination ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*destination ipv4 start*> <*destination ipv4 end*>.

   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.

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

   If `any` is specified, the destination IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the destination IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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.

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 4-3: Port names that can be specified for TCP* and *Table 4-4: Port names that can be specified for UDP (IPv4)*.

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

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

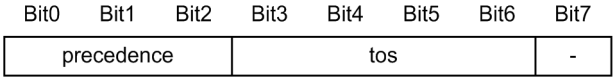
If `range` is specified, the filter condition is in the range from <*destination port start*> to <*destination port end*>.

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:

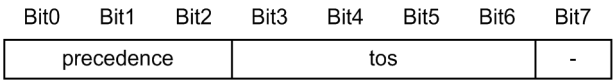
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 4-6: 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:

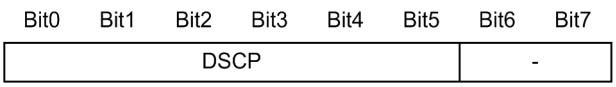
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 4-7: 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 4-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 4-11: 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 when 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.

Fragments

Specifies the second and subsequent fragmented packets.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

  action

  To set or change an action parameter, you must set the `action` parameter keyword at the

beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

log

The packets discarded by the specified access list are included in access list logging.

1. Default value when this parameter is omitted:

   None. (Access list logging is not used.)

2. Range of values:

   None

Default behavior

None

Impact on communication

If an entry is added or 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 *nnn.nnn.nnn.nnn* `0.0.0.0` is entered as the source address and the destination address, `host` *nnn.nnn.nnn.nnn* is displayed.

Related commands

access-list

ip access-group

ip access-list resequence

permit (ip access-list extended)

remark

vlan-list

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} [<*action-specification*>]

Action specification

action log

To delete information:

no <*sequence*>

Input mode

`(config-std-nacl)`

Parameters

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

   Note, however, that if the maximum value for the application sequence 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.

To specify all IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*ipv4*> `[`<*ipv4 wildcard*>`]`, `host` <*ipv4*>, or `any`.

   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*>.

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

   If `any` is specified, IPv4 addresses are not used as a filter condition.

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

- Action parameters

  action

  To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

  1. Default value when this parameter is omitted:

     None. (This `action` parameter keyword cannot be omitted if an action is set.)

  2. Range of values:

     None

  log

  The packets discarded by the specified access list are included in access list logging.

  1. Default value when this parameter is omitted:

     None. (Access list logging is not used.)

  2. Range of values:

     None

Default behavior

None

Impact on communication

If an entry is added or 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. When *nnn*`.`*nnn*`.`*nnn*`.`*nnn* `0.0.0.0` is entered as the address, `host` *nnn*`.`*nnn*`.`*nnn*`.`*nnn* is displayed.

Related commands

access-list

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.

Syntax

To set or change information:

[<*sequence*>] deny {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

- When the upper-layer protocol is other than TCP, UDP, and ICMP

  {ipv6 | <*protocol*>} {<*source ipv6*>/<*length*> | host <*source ipv6*> | any | own-address <*own address length*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is TCP

  tcp {<*source ipv6*>/<*length*> | host <*source ipv6*> | 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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}][{[established] | [{ack|+ack|-ack}] [{fin|+fin|-fin}] [{psh|+psh|-psh}] [{rst|+rst|-rst}] [{syn|+syn|-syn}] [{urg|+urg|-urg}]}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is UDP

  udp {<*source ipv6*>/<*length*> | host <*source ipv6*> | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is ICMP

  icmp {<*source ipv6*>/<*length*> | host <*source ipv6*> | any | own-address <*own address length*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

Action specification

action log

To delete information:

no <*sequence*>

Input mode

`(config-ipv6-acl)`

Parameters

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{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 4-2: Protocol names that can be specified (IPv6)*.

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

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv6*>/<*length*>, `host` <*source ipv6*>, `own-address` <*own address length*>, or `any`.

   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.

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

   If `any` is specified, the source IPv6 address is not used as a filter condition.

   `own-address` is valid only for the `traffic-filter` command for a VLAN interface.

   If `own-address` is specified, the filter condition is the source IPv6 address that has been set as the IPv6 global address on the target interface.

   <*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.

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 4-3: Port names that can be specified for TCP* and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

   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*>.

   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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv6*>/<*length*>, `own-address` <*own address length*>, `host` <*destination ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*destination ipv6 start*> <*destination ipv6 end*>.

   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 `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

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

   If `any` is specified, the destination IPv6 address is not used as a filter condition.

   `own-address` and `own` are valid only for the `traffic-filter` command for a VLAN interface.

   `range-address` is valid only for the `traffic-filter` command for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the destination IPv6 address that has been set as the IPv6 global address on the target interface.

   If `own` is specified, the filter conditions are the destination IPv6 address that has been set

as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

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.

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 4-3: Port names that can be specified for TCP* and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

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

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

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

   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.)

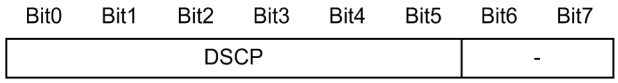
2. Range of values:

   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 4-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 4-12: 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

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

log

The packets discarded by the specified access list are included in access list logging.

1. Default value when this parameter is omitted:

   None. (Access list logging is not used.)

2. Range of values:

   None

Default behavior

None

Impact on communication

If an entry is added or 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*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*/0 is entered as the source address and the destination address, any is displayed.
2. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*/128 is entered as the source address and the destination address, host *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn* is displayed.

Related commands

ipv6 traffic-filter

ipv6 access-list resequence

permit (ipv6 access-list)

remark

vlan-list

deny (mac access-list extended)

Specifies the conditions by which the MAC filter denies access.

Syntax

To set or change information:

[<*sequence*>] deny {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

{<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol } [<*ethernet type*>] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

Action specification

action log

To delete information:

no <*sequence*>

Input mode

`(config-ext-macl)`

Parameters

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the source MAC address.

To specify all source MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source mac*> <*source mac mask*>, `host` <*source mac*>, or `any`.

   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.

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

If `any` is specified, the source MAC address is not used as a filter condition.

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

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol}

Specifies the destination MAC address.

To specify all destination MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination mac*> <*destination mac mask*>, `host` <*destination mac*>, `any`, `bpdu`, `cdp`, `lacp`, `lldp`, `oadp`, `pvst-plus-bpdu`, or `slow-protocol`.

   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.

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

   If `any` is specified, the destination MAC address is not used as a filter condition.

   If `bpdu` is specified, BPDU control packets are used as the filter condition.

   If `cdp` is specified, CDP control packets are used as the filter condition.

   If `lacp` or `slow-protocol` is specified, slow protocol packets are used as the filter condition.

   This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD functionality.

   If `lldp` is specified, LLDP control packets are used as the filter condition.

   If `oadp` is specified, OADP control packets are used as the filter condition.

   If `pvst-plus-bpdu` is specified, PVST+ control packets are used as the filter condition.

   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 4-9: Ethernet type names that can be specified*.

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

Specify the VLAN ID or VLAN list name.

For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

log

The packets discarded by the specified access list are included in access list logging.

1. Default value when this parameter is omitted:

   None. (Access list logging is not used.)

2. Range of values:

   None

Default behavior

None

Impact on communication

If an entry is added or 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 a protocol name is set for the destination address or if the address of a protocol name that can be set is set, the protocol name is displayed. For details about the address of a protocol name that can be specified as the destination address, see *Table 4-10: Destination MAC address names that can be specified*. 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

vlan-list

ip access-group

Applies an IPv4 access list to an Ethernet interface or a VLAN interface, and enables the IPv4 filtering functionality.

For details about the number of specifications that can be set for an interface, see *Number of specifications that can be set for an interface*.

When an access list with the parameter specifying policy-based routing set is applied to an interface, specify the inbound side of the VLAN interface, and Layer 3 forwarding as the forwarding type.

If you apply an access list with the policy-based routing parameter specified, specify the inbound side of the VLAN interface.

Syntax

To set information:

- Ethernet interface

  ip access-group {<*access list number*> | <*access list name*>} {in | out} layer2-forwarding

- VLAN interface

  ip access-group {<*access list number*> | <*access list name*>} {in | out} {layer2-forwarding | layer3-forwarding}

To delete information:

- Ethernet interface

  no ip access-group {<*access list number*> | <*access list name*>} {in | out} layer2-forwarding

- VLAN interface

  no ip access-group {<*access list number*> | <*access list name*>} {in | out} {layer2-forwarding | layer3-forwarding}

Input mode

`(config-if)`

Parameters

{<*access list number*>|<*access list name*>}

Specifies the identifier of the IPv4 address filter or the IPv4 packet filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*access list number*>, specify values from 1 to 199, or from 1300 to 2699 (in decimal).

   For <*access list name*>, specify a name that is 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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{layer2-forwarding | layer3-forwarding}

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

`layer3-forwarding` detects IP packets forwarded on Layer 3 in flow detection.

This parameter has an effect only when it is applied to a VLAN interface.

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 applied to an interface, IP packets received at the interface are 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. On an Ethernet interface, you can set one IPv4 filter for each of Inbound and Outbound.

   On a VLAN interface, you can set one IPv4 filter for each of Inbound Layer 2 forwarding, Inbound Layer 3 forwarding, Outbound Layer 2 forwarding, and Outbound Layer 3 forwarding.

   If a filter has already been set, first remove it and then set it again.

2. If you specify a non-existent IPv4 filter, this will be ignored. The identifier of the IPv4 filter is registered.

3. You can set an IPv4 access list if the flow distribution pattern is `default standard`, `default standard-advance`, `default extended`, `default extended-advance`, `filter-only`

`extended`, `filter-only extended-advance`, `filter extended`, `filter extended-advance`, `qos extended`, or `qos extended-advance`.

4. When the `own-address` or `own` parameter is specified in the flow detection condition, you can set an IPv4 access list if an IPv4 address is set for the target interface.
5. When an Advance access list is to be applied to an Ethernet interface and a VLAN parameter is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.
6. When an IPv4 access list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.
7. When an IPv4 access list is to be applied to an Ethernet interface and the Layer 2 forwarding of a VLAN interface, you can set the list if neither TCP flag nor tos parameter is set in the flow detection condition.
8. When an IPv4 access list is to be applied to the Layer 2 forwarding of a VLAN interface, you can set the list if MAC mode is not set.
9. Before specifying `log` as an action in an access list, enable logging by using the `system hardware-mode` command with the `access-log` parameter.

Related commands

access-list

ip access-list standard

ip access-list extended

ip access-list extended

Configures an access list to serve 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.

An IPv4 packet filter filters based on source IPv4 address, destination IPv4 address, VLAN ID, user priority, fragmented packet, ToS field value, port number, TCP flag, ICMP type, ICMP code, and IGMP type.

You can use one access list ID and specify multiple filter conditions.

For details of the number of access lists and filter conditions that can be created for a Switch, see *Number of access lists that can be created*.

If you specify `permit` for the filter action, you can specify parameters for policy-based routing. In this case, if you use access group commands to apply the target access list to an interface, specify the inbound side of the VLAN interface, and Layer 3 forwarding as the forwarding type.

If you specify `permit` for the filter action, you can specify parameters for policy-based switching. If you use access group commands to apply the target access list to an interface, specify the inbound side of the Ethernet interface.

Syntax

To set information:

ip access-list extended {<*access list number*> | <*access list name*>}

To delete information:

no ip access-list extended {<*access list number*> | <*access list name*>}

Input mode

`(config)`

Parameters

{<*access list number*> | <*access list name*>}

Specifies the identifier of the IPv4 packet filter that is to be set.

The Switch enters `config-ext-nacl` mode.

Names that have already been used for IPv4 address filters, IPv6 filters, MAC filters, and Advance filters cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*access list number*>, specify values from 100 to 199, or from 2000 to 2699 (in decimal).

   For <*access list name*>, specify a name that is 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

1. For <*access list number*>, you can use 100 to 199 or 2000 to 2699 in the `access-list` command.
2. You cannot specify IPv4 address filter names, IPv6 access list names, and MAC access list names that have already been created.

Related commands

access-list

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 filter conditions.

Syntax

To set or change information:

ip access-list resequence {<*access list number*> | <*access list name*>} [<*starting sequence*> [<*increment sequence*>]]

Input mode

(config)

Parameters

{<*access list number*> | <*access list name*>}

Specifies the identifier of the IPv4 address filter or the IPv4 packet filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*access list number*>, specify a number from 1 to 199, or from1300 to 2699 (in decimal).

   For <*access list name*>, specify a name that is 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

access-list

ip access-list standard

ip access-list extended

ip access-list standard

Configures an access list to serve 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.

An IPv4 address filter filters packets based on IPv4 address.

You can use one access list ID and specify multiple filter conditions.

For details of the number of access lists and filter conditions that can be created for a Switch, see *Number of access lists that can be created*.

Syntax

To set information:

ip access-list standard {<*access list number*> | <*access list name*>}

To delete information:

no ip access-list standard {<*access list number*> | <*access list name*>}

Input mode

`(config)`

Parameters

{<*access list number*> | <*access list name*>}

Specifies the identifier of the IPv4 address filter that is to be set.

The Switch enters `config-std-nacl` mode.

Names that have already been used for IPv4 packet filters, IPv6 filters, MAC filters, and Advance filters cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*access list number*>, specify values from 1 to 99, or from 1300 to 1999 (in decimal).

   For <*access list name*>, specify a name that is 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

1. For <*access list number*>, you can use 1 to 99 or 1300 to 1999 in the `access-list` command.
2. You cannot specify IPv4 packet filter names, IPv6 access list names, and MAC access list names that have already been created.

Related commands

access-list

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. An access list used for an IPv6 filter filters packets based on source IPv6 address, destination IPv6 address, VLAN ID, user priority, traffic class field value, port number, TCP flag, ICMP type, and ICMP code.

You can use one access list ID and specify multiple filter conditions.

For details of the number of access lists and filter conditions that can be created for a Switch, see *Number of access lists that can be created*.

If you specify `permit` for the filter action, you can specify parameters for policy-based routing. In this case, if you use access group commands to apply the target access list to an interface, specify the inbound side of the VLAN interface, and Layer 3 forwarding as the forwarding type.

If you specify `permit` for the filter action, you can specify parameters for policy-based switching. If you use access group commands to apply the target access list to an interface, specify the inbound side of the Ethernet interface.

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 identifier of the IPv6 filter that is to be set.

The Switch enters `config-ipv6-acl` mode.

Names that have already been used for IPv4 address filters, IPv4 packet filters, MAC filters, and Advance filters cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

1. You cannot specify IPv4 packet filter names, IPv4 address filter names, and MAC access list

names that have already been created.

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 filter 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 identifier of the IPv6 filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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 Ethernet interface or VLAN interface and enables IPv6 filtering.

For details about the number of specifications that can be set for an interface, see *Number of specifications that can be set for an interface*.

When an access list with the parameter specifying policy-based routing set is applied to an interface, specify the inbound side of the VLAN interface, and Layer 3 forwarding as the forwarding type.

If you apply an access list with the policy-based routing parameter specified, specify the inbound side of the VLAN interface.

Syntax

To set information:

- Ethernet interface

  ipv6 traffic-filter <*access list name*> {in | out} layer2-forwarding

- VLAN interface

  ipv6 traffic-filter <*access list name*> {in | out} {layer2-forwarding | layer3-forwarding}

To delete information:

- Ethernet interface

  no ipv6 traffic-filter <*access list name*> {in | out} layer2-forwarding

- VLAN interface

  no ipv6 traffic-filter <*access list name*> {in | out} {layer2-forwarding | layer3-forwarding}

Input mode

`(config-if)`

Parameters

<*access list name*>

Specifies the identifier of the IPv6 filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{layer2-forwarding | layer3-forwarding}

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

`layer3-forwarding` detects IP packets forwarded on Layer 3 in flow detection.

This parameter has an effect only when it is applied to a VLAN interface.

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 applied to an interface, IPv6 packets received at the interface are 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. On an Ethernet interface, you can set one IPv6 filter for each of Inbound and Outbound.

   On a VLAN interface, you can set one IPv6 filter for each of Inbound Layer 2 forwarding, Inbound Layer 3 forwarding, Outbound Layer 2 forwarding, and Outbound Layer 3 forwarding.

   If a filter has already been set, first remove it and then set it again.

2. If a non-existent IPv6 filter is set, no action is performed. The identifier of the IPv6 filter is registered.

3. You can set an IPv6 access list if the flow distribution pattern is `default standard`, `default standard-advance`, `default extended`, `default extended-advance`, `filter-only extended`, `filter-only extended-advance`, `filter extended`, `filter extended-advance`, `qos extended`, or `qos extended-advance`.

4. If the distribution pattern of path-related table entries is `ipv4-uni standard` or `ipv4-uni extended`, you cannot set an IPv6 access list with IPv6 policy-based routing specified.

   You can set it if the distribution pattern of path-related table entries is other than above.

5. When the `own-address` or `own` parameter is specified in the flow detection condition, you can set an IPv6 access list if one IPv6 global address only is set for the target interface.
6. You can set an IPv6 access list if, for the source address which is a parameter in the flow detection condition, `any` is specified or a value no more than 64 is specified for `Len`.
7. When an Advance access list is to be applied to an Ethernet interface and a VLAN parameter is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.
8. When an IPv6 access list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.
9. When an IPv6 access list is to be applied to an Ethernet interface and the Layer 2 forwarding of a VLAN interface, you can set the list if neither the TCP flag nor traffic class field parameter is set in the flow detection condition.
10. When an IPv6 access list is to be applied to the Layer 2 forwarding of a VLAN interface, you can set the list if MAC mode is not set.
11. Before specifying `log` as an action in an access list, enable logging by using the `system hardware-mode` command with the `access-log` parameter.

Related commands

ipv6 access-list

mac access-group

Applies a MAC access list to an Ethernet interface or a VLAN interface and enables the MAC filtering functionality.

For details about the number of specifications that can be set for an interface, see *Number of specifications that can be set for an interface*.

If you apply an access list with the policy-based routing parameter specified, specify the inbound side of the VLAN interface.

Syntax

To set information:

mac access-group <*access list name*> {in | out} layer2-forwarding

To delete information:

no mac access-group <*access list name*> {in | out} layer2-forwarding

Input mode

`(config-if)`

Parameters

<*access list name*>

Specifies the identifier of the MAC filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects non-IP packets forwarded on Layer 2 in flow detection.

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 applied to an interface, all packets received at the interface are 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. On an interface, you can set one MAC filter for each of Inbound and Outbound. If a filter has already been set, first remove it and then set it again.
2. If you specify a non-existent MAC filter, this will be ignored. The identifier of a MAC access list is registered.
3. You can set a MAC access list if the flow distribution pattern is `default standard`, `default standard-advance`, `default extended`, `default extended-advance`, `filter-only extended`, `filter-only extended-advance`, `filter extended`, `filter extended-advance`, `qos extended`, or `qos extended-advance`.
4. When an Advance access list is to be applied to an Ethernet interface and a VLAN parameter is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.
5. When a MAC access list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.
6. Before specifying `log` as an action in an access list, enable logging by using the `system hardware-mode` command with the `access-log` parameter.

Related commands

mac access-list extended

mac access-list extended

Sets an access list to be used in a MAC filter. An access list used for a MAC filter filters packets based on source MAC address, destination MAC address, Ethernet type number, VLAN ID, and user priority.

You can use one access list ID and specify multiple filter conditions.

For details of the number of access lists and filter conditions that can be created for a Switch, see *Number of access lists that can be created*.

If you specify `permit` for the filter action, you can specify parameters for policy-based switching. If you use access group commands to apply the target access list to an interface, specify the inbound side of the Ethernet interface.

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 identifier of the MAC filter that is to be set.

The Switch enters `config-ext-macl` mode.

Names that have already been used for IPv4 address filters, IPv4 packet filters, IPv6 filters, and Advance filters cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

1. You cannot specify IPv4 packet filter names, IPv4 address filter names, and IPv6 access list names that have already been created.

Related commands

mac access-group

mac access-list resequence

deny (mac access-list extended)

permit (mac access-list extended)

remark

mac access-list resequence

Resets the sequence number for the order in which the filter conditions in a MAC filter are applied.

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 identifier of the MAC filter that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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 {<*filter-condition*>} [<*action-specification*>]

[<*sequence*>] permit mac-ip {<*filter-condition*>} [<*action-specification*>]

[<*sequence*>] permit mac-ipv6 {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

For `mac` {<*filter-condition*>}:

This filter 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} [<*ethernet type*>][vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

For `mac-ip` {<*filter-condition*>}:

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

- When "packet is not fragmented" is a condition, and the upper-layer protocol is 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ip | <*protocol*>} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} tcp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} igmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [<*igmp type*>] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When "packet is fragmented" is a condition

  mac-ip {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [fragments] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

For `mac-ipv6 {`<*filter-condition*>`}`:

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

- When the upper-layer protocol is 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ipv6 | <*protocol*>} {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*source ipv6 start*> <*source ipv6 end*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} tcp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any| own-address <*own address length*> | own | 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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} udp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} icmp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*source ipv6 start*> <*source ipv6 end*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority

<*priority*>] [ctag-vlan <*vlan id*>]}]

Action specification

For `mac` {<*filter-condition*>}:

action policy-switch-list <*policy switch list no.*>

For `mac-ip` {<*filter-condition*>}:

action {policy interface vlan <*vlan id*> next-hop <*next hop ipv4*> | policy-list <*policy list no.*> | policy-switch-list <*policy switch list no.*>}

For `mac-ipv6` {<*filter-condition*>}:

action {policy interface vlan <*vlan id*> next-hop <*next hop ipv6*> | policy-switch-list <*policy switch list no.*>}

To delete information:

no <*sequence*>

Input mode

`(config-adv-acl)`

Parameters

<*sequence*>

Sets the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

- Filter condition parameters

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

Specifies the source MAC address.

To specify all source MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source mac*> <*source mac mask*>, `host` <*source mac*>, or `any`.

   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.

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

   If `any` is specified, the source MAC address is not used as a filter condition.

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

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol}

Specifies the destination MAC address.

To specify all destination MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination mac*> <*destination mac mask*>, `host` <*destination mac*>, `any`, `bpdu`, `cdp`, `lacp`, `lldp`, `oadp`, `pvst-plus-bpdu`, or `slow-protocol`.

   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.

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

   If `any` is specified, the destination MAC address is not used as a filter condition.

   If `bpdu` is specified, BPDU control packets are used as the filter condition.

   If `cdp` is specified, CDP control packets are used as the filter condition.

   If `lacp` or `slow-protocol` is specified, slow protocol packets are used as the filter condition.

   This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD functionality.

   If `lacp` is specified, LACP control packets are used as the filter condition.

   If `lldp` is specified, LLDP control packets are used as the filter condition.

   If `oadp` is specified, OADP control packets are used as the filter condition.

   If `pvst-plus-bpdu` is specified, PVST+ control packets are used as the filter condition.

   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 4-9: Ethernet type names that can be specified*.

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

For details about the VLAN ID, see *Specifiable values for parameters*.

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.

ctag-untagged

Specifies detection of packets with no customer tag.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

ctag-user-priority <*priority*>

Specifies a user priority for the customer 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.

ctag-vlan <*vlan id*>

Specifies a VLAN ID for the customer 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 4-1: 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 4-2: Protocol names that can be specified (IPv6)*.

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

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv4*> <*source ipv4 wildcard*>, `host` <*source ipv4*>, `any`, `own-address` <*source ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*source ipv4 start*> <*source ipv4 end*>.

   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.

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

   If `any` is specified, the source IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the source IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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 | range-address <*source ipv6 start*> <*source ipv6 end*>}

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv6*>/<*length*>, `own-address` <*own address length*>, `host` <*source ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*source ipv6 start*> <*source ipv6 end*>.

   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.

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

   If `any` is specified, the source IPv6 address is not used as a filter condition.

   `own-address` and `own` are valid only for the `traffic-filter` command for a VLAN interface.

   `range-address` is valid only for the `traffic-filter` command for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the source IPv6 address that has been set as the IPv6 global address on the target interface.

   If `own` is specified, the filter conditions are the source IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

   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.

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 4-3: Port names that can be specified for TCP*, *Table 4-4: Port names that can be specified for UDP (IPv4)*, and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

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

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

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

   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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv4*> <*destination ipv4 wildcard*>, `host` <*destination ipv4*>, `any`, `own-address` <*destination ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*destination ipv4 start*> <*destination ipv4 end*>.

   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.

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

   If `any` is specified, the destination IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the destination IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv6*>/<*length*>, `own-address` <*own address length*>, `host` <*destination ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*destination ipv6 start*> <*destination ipv6 end*>.

   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 `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

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

If `any` is specified, the destination IPv6 address is not used as a filter condition.

`own-address` and `own` are valid only for the `traffic-filter` command for a VLAN interface.

`range-address` is valid only for the `traffic-filter` command for an Ethernet interface or a VLAN interface.

If `own-address` is specified, the filter condition is the destination IPv6 address that has been set as the IPv6 global address on the target interface.

If `own` is specified, the filter conditions are the destination IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

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.

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 4-3: Port names that can be specified for TCP*, *Table 4-4: Port names that can be specified for UDP (IPv4)*, and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

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

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

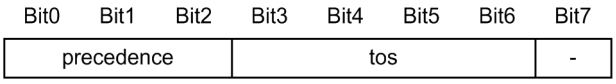
   If `range` is specified, the filter condition is in the range from <*destination port start*> to <*destination port end*>.

   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:

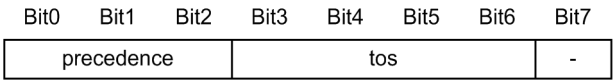
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 4-6: 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 4-7: 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:

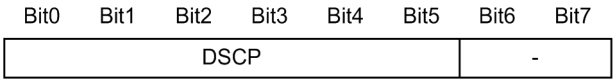
   Specify 0 to 255 in decimal.

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.

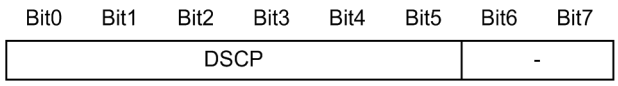
Its value is compared with the first 6 bits in the ToS field of the received packet.



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 six 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 4-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 4-11: Message names that can be specified for ICMP (IPv4)* and *Table 4-12: 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 when 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.

Fragments

Specifies the second and subsequent fragmented packets.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

- Action parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

policy interface vlan <*vlan id*> next-hop <*next hop ipv4*>

Specifies the output destination for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   <vlan id>

   For details about the VLAN ID, see *Specifiable values for parameters*.

   <next hop ipv4>

   Specifies a next-hop IPv4 address.

   Specify an address in the network that connects to the specified destination interface. However, you cannot specify the direct broadcast address of the network connected to the specified destination interface or an address that has been set on the specified destination interface.

policy interface vlan *<vlan id>* next-hop *<next hop ipv6>*

Specifies the output destination for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   <vlan id>

   For details about the VLAN ID, see *Specifiable values for parameters*.

   For the VLAN interface specified by the VLAN ID, `ipv6 enable` must be set and the IPv6 functionality must be enabled.

   <next hop ipv6>

   Specifies a next-hop IPv6 address.

   Specify an address in the network that connects to the specified destination interface. However, you cannot specify an address that has been set on the specified destination interface

policy-list *<policy list no.>*

Specifies the list number for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   Specify the list number for policy-based routing that was set by using the `policy-list` command.

policy-switch-list *<policy switch list no.>*

Specifies the list number for policy-based switching.

1. Default value when this parameter is omitted:

   None. (Policy-based switching is not used.)

2. Range of values:

   Specify the list number for policy-based switching that was set by using the `policy-switch-list` command.

Default behavior

None

Impact on communication

If an entry is added or 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 a protocol name is set for the destination MAC address, or if the address of a protocol name that can be set is set, the protocol name is displayed. For details about the address of a protocol name that can be specified as the destination MAC address, see *Table 4-10: Destination MAC address names that can be specified*.

   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. When `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 *nnn*.*nnn*.*nnn*.*nnn* `0.0.0.0` is entered as the source IPv4 address and the destination IPv4 address, `host` *nnn*.*nnn*.*nnn*.*nnn* is displayed.
5. If policy-based routing is specified for the action parameter, the following addresses cannot be specified for the source IPv4 address and destination IPv4 address that are set for filtering conditions:

   Source IPv4 address

   Multicast address and internal loopback address

   Destination IPv4 address

   Multicast address, restricted broadcast address, and internal loopback address
6. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/0` is entered as the source IPv6 address and the destination IPv6 address, `any` is displayed.
7. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/128` is entered as the source IPv6 address and the destination IPv6 address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn* is displayed.
8. If policy-based routing is specified for the action parameter, multicast addresses and link-local addresses cannot be specified for the source IPv6 address and destination IPv6 address that are set for filtering conditions.
9. If policy-based switching is specified for the action parameter, specify the VLAN ID set in the specified policy-based switching list for `vlan` of the filter condition parameters. Note that you cannot specify a VLAN list name at this time.

Related commands

advance access-group

advance access-list resequence

deny (advance access-list)

remark

vlan-list

policy-list

policy-switch-list

permit (ip access-list extended)

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

Note that input format is different if you specify fragmented packets as the detection condition. See *When "packet is fragmented" is a condition* of *Syntax*.

Syntax

To set or change information:

[<*sequence*>] permit {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

- When the upper-layer protocol is other than TCP, UDP, ICMP, and IGMP

  {ip | <*protocol*>} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is TCP

  tcp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack|+ack|-ack}] [{fin|+fin|-fin}] [{psh|+psh|-psh}] [{rst|+rst|-rst}] [{syn|+syn|-syn}] [{urg|+urg|-urg}]}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is UDP

  udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is ICMP

  icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is IGMP

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

{{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [<*igmp type*>] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When "packet is fragmented" is a condition

  {ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [fragments] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

Action specification

action {policy interface vlan <*vlan id*> next-hop <*next hop ipv4*> | policy-list <*policy list no.*> | policy-switch-list <*policy switch list no.*>}

To delete information:

no <*sequence*>

Input mode

`(config-ext-nacl)`

Parameters

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

■ Filter condition parameters

{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 4-1: Protocol names that can be specified (IPv4)*.

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

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv4*> <*source ipv4 wildcard*>, `host` <*source ipv4*>, `any`, `own-address` <*source ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*source ipv4 start*> <*source ipv4 end*>.

   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.

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

   If `any` is specified, the source IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the source IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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.

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 4-3: Port names that can be specified for TCP* and *Table 4-4: Port names that can be specified for UDP (IPv4)*.

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

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

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

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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv4*> <*destination ipv4 wildcard*>, `host` <*destination ipv4*>, `any`, `own-address` <*destination ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*destination ipv4 start*> <*destination ipv4 end*>.

   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.

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

   If `any` is specified, the destination IPv4 address is not used as a filter condition.

   `own-address` and `own` are valid only for `access-group` commands for a VLAN interface.

   `range-address` is valid only for `access-group` commands for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the destination IPv4 address that has been set on the target interface.

   If `own` is specified, the filter condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the filter condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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.

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 4-3: Port names that can be specified for TCP* and *Table 4-4: Port names that can be specified for UDP (IPv4)*.

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

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

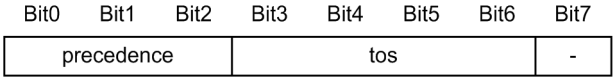
If `range` is specified, the filter condition is in the range from <*destination port start*> to <*destination port end*>.

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:

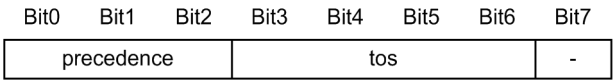
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 4-6: 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:

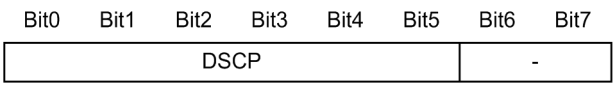
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 4-7: 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 4-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 4-11: 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 when 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.

Fragments

Specifies the second and subsequent fragmented packets.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the

beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

policy interface vlan <*vlan id*> next-hop <*next hop ipv4*>

Specifies the output destination for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   <*vlan id*>

   For details about the VLAN ID, see *Specifiable values for parameters*.

   <*next hop ipv4*>

   Specifies a next-hop IPv4 address.

   Specify an address in the network that connects to the specified destination interface. However, you cannot specify the direct broadcast address of the network connected to the specified destination interface or an address that has been set on the specified destination interface.

policy-list <*policy list no.*>

Specifies the list number for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   Specify the list number for policy-based routing that was set by using the `policy-list` command.

policy-switch-list <*policy switch list no.*>

Specifies the list number for policy-based switching.

1. Default value when this parameter is omitted:

   None. (Policy-based switching is not used.)

2. Range of values:

   Specify the list number for policy-based switching that was set by using the `policy-switch-list` command.

Default behavior

None

Impact on communication

If an entry is added or 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 *nnn*`.` *nnn*`.` *nnn*`.` *nnn* `0.0.0.0` is entered as the source address and the destination address, `host` *nnn*`.` *nnn*`.` *nnn*`.` *nnn* is displayed.
3. If policy-based routing is specified for the action parameter, the following addresses cannot be specified for the source IPv4 address and destination IPv4 address that are set for filtering conditions:

   Source IPv4 address

   Multicast address and internal loopback address

   Destination IPv4 address

   Multicast address, restricted broadcast address, and internal loopback address
4. If policy-based switching is specified for the action parameter, specify the VLAN ID set in the specified policy-based switching list for `vlan` of the filter condition parameters. Note that you cannot specify a VLAN list name at this time.

Related commands

access-list

ip access-group

ip access-list resequence

deny (ip access-list extended)

remark

vlan-list

policy-list

policy-switch-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 in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

   Note, however, that if the maximum value for the application sequence 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}

Specifies the IPv4 address.

To specify all IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*ipv4*> `[`<*ipv4 wildcard*>`]`, `host` <*ipv4*>, or `any`.

   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*>.

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

   If `any` is specified, IPv4 addresses are not used as a filter condition.

   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 added or 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. When *nnn*`.`*nnn*`.`*nnn*`.`*nnn* `0.0.0.0` is entered as the address, `host` *nnn*`.`*nnn*`.`*nnn*`.`*nnn* is displayed.

Related commands

access-list

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.

Syntax

To set or change information:

[<*sequence*>] permit {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

- When the upper-layer protocol is other than TCP, UDP, and ICMP

  {ipv6 | <*protocol*>} {<*source ipv6*>/<*length*> | host <*source ipv6*> | any | own-address <*own address length*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is TCP

  tcp {<*source ipv6*>/<*length*> | host <*source ipv6*> | 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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is UDP

  udp {<*source ipv6*>/<*length*> | host <*source ipv6*> | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- When the upper-layer protocol is ICMP

  icmp {<*source ipv6*>/<*length*> | host <*source ipv6*> | any | own-address <*own address length*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

Action specification

action {policy interface vlan <*vlan id*> next-hop <*next hop ipv6*>| policy-switch-list <*policy switch list no.*>}

To delete information:

no <*sequence*>

Input mode

`(config-ipv6-acl)`

Parameters

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

- Filter condition parameters

{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 4-2: Protocol names that can be specified (IPv6)*.

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

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv6*>/<*length*>, `host` <*source ipv6*>, `own-address` <*own address length*>, or `any`.

   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.

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

   If `any` is specified, the source IPv6 address is not used as a filter condition.

   `own-address` is valid only for the `traffic-filter` command for a VLAN interface.

   If `own-address` is specified, the filter condition is the source IPv6 address that has been set as the IPv6 global address on the target interface.

<*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.

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 4-3: Port names that can be specified for TCP* and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

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

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

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

   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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv6*>/<*length*>, `own-address` <*own address length*>, `host` <*destination ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*destination ipv6 start*> <*destination ipv6 end*>.

   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 `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

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

   If `any` is specified, the destination IPv6 address is not used as a filter condition.

   `own-address` and `own` are valid only for the `traffic-filter` command for a VLAN interface.

   `range-address` is valid only for the `traffic-filter` command for an Ethernet interface or a VLAN interface.

   If `own-address` is specified, the filter condition is the destination IPv6 address that has been set as the IPv6 global address on the target interface.

If `own` is specified, the filter conditions are the destination IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

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.

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 4-3: Port names that can be specified for TCP* and *Table 4-5: Port names that can be specified for UDP (IPv6)*.

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

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

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

   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.)

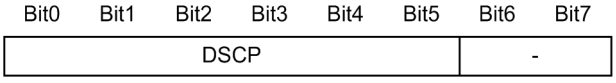
2. Range of values:

   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 4-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 4-12: 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

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

policy interface vlan <*vlan id*> next-hop <*next hop ipv6*>

Specifies the output destination for policy-based routing.

1. Default value when this parameter is omitted:

   None. (Policy-based routing is not used.)

2. Range of values:

   <*vlan id*>

For details about the VLAN ID, see *Specifiable values for parameters*.

For the VLAN interface specified by the VLAN ID, `ipv6 enable` must be set and the IPv6 functionality must be enabled.

<next hop ipv6>

Specifies a next-hop IPv6 address.

Specify an address in the network that connects to the specified destination interface. However, you cannot specify an address that has been set on the specified destination interface

policy-switch-list *<policy switch list no.>*

Specifies the list number for policy-based switching.

1. Default value when this parameter is omitted:

   None. (Policy-based switching is not used.)

2. Range of values:

   Specify the list number for policy-based switching that was set by using the `policy-switch-list` command.

Default behavior

None

Impact on communication

If an entry is added or 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*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/0` is entered as the source address and the destination address, `any` is displayed.
2. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/128` is entered as the source address and the destination address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn* is displayed.
3. If policy-based routing is specified for the action parameter, multicast addresses and link-local addresses cannot be specified for the source IPv6 address and destination IPv6 address that are set for filtering conditions.
4. If policy-based switching is specified for the action parameter, specify the VLAN ID set in the specified policy-based switching list for `vlan` of the filter condition parameters. Note that you cannot specify a VLAN list name at this time.

Related commands

ipv6 traffic-filter

ipv6 access-list resequence

deny (ipv6 access-list)

remark

vlan-list

policy-switch-list

permit (mac access-list extended)

Specifies the conditions by which the MAC filter permits access.

Syntax

To set or change information:

[<*sequence*>] permit {<*filter-condition*>} [<*action-specification*>]

<*filter-condition*>

{<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol } [<*ethernet type*>] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

Action specification

action policy-switch-list <*policy switch list no.*>

To delete information:

no <*sequence*>

Input mode

`(config-ext-macl)`

Parameters

<*sequence*>

Specifies the sequence in which filter 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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

- Filter condition parameters

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

Specifies the source MAC address.

To specify all source MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source mac*> <*source mac mask*>, `host` <*source mac*>, or `any`.

   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.

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

If `any` is specified, the source MAC address is not used as a filter condition.

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

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol }

Specifies the destination MAC address.

To specify all destination MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination mac*> <*destination mac mask*>, `host` <*destination mac*>, `any`, `bpdu`, `cdp`, `lacp`, `lldp`, `oadp`, `pvst-plus-bpdu`, or `slow-protocol`.

   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.

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

   If `bpdu` is specified, BPDU control packets are used as the filter condition.

   If `cdp` is specified, CDP control packets are used as the filter condition.

   If `lacp` or `slow-protocol` is specified, slow protocol packets are used as the filter condition.

   This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD functionality.

   If `lldp` is specified, LLDP control packets are used as the filter condition.

   If `oadp` is specified, OADP control packets are used as the filter condition.

   If `pvst-plus-bpdu` is specified, PVST+ control packets are used as the filter condition.

   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 4-9: Ethernet type names that can be specified*.

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

policy-switch-list <*policy switch list no.*>

Specifies the list number for policy-based switching.

1. Default value when this parameter is omitted:

   None. (Policy-based switching is not used.)

2. Range of values:

   Specify the list number for policy-based switching that was set by using the `policy-switch-list` command.

Default behavior

None

Impact on communication

If an entry is added or 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 a protocol name is set for the destination address or if the address of a protocol name that can be set is set, the protocol name is displayed. For details about the address of a protocol name that can be specified as the destination address, see *Table 4-10: Destination MAC address names that can be specified*. 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.

3. If policy-based switching is specified for the action parameter, specify the VLAN ID set in the specified policy-based switching list for `vlan` of the filter condition parameters. Note that the VLAN list name cannot be specified

Related commands

mac access-group

mac access-list resequence

deny (mac access-list extended)

remark

vlan-list

policy-switch-list

remark

Specifies supplementary information for the 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:

   The initial value is null.

2. Range of values:

   Enclose a character string of no more than 64 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

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

5. Access List Logging

access-log enable
access-log interval
access-log rate-limit
access-log threshold

access-log enable

Enables access list logging.

Syntax

To set information:

access-log enable

To delete information:

no access-log enable

Input mode

`(config)`

Parameters

None

Default behavior

Access list logging is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To configure this, first enter the `system hardware-mode` command with the `access-log` parameter.

Related commands

access-list

deny (advance access-list)

deny (ip access-list extended)

deny (ip access-list standard)

deny (ipv6 access-list)

deny (mac access-list extended)

system hardware-mode

access-log interval

Specifies the interval for outputting access list logs for access list logging.

Syntax

To set information:

access-log interval {<*minutes*> | unlimit}

To delete information:

no access-log interval

Input mode

`(config)`

Parameters

{<*minutes*> | unlimit}

Specifies the interval for outputting access list logs.

<*minutes*>

Specifies the interval in minutes.

unlimit

Specifies that access list log output is not triggered at a preset time interval. To check the managed access list log information, use the `show access-log flow` operation command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   5 to 1440 (24 hours), or unlimit

Default behavior

Access list logs are output at five-minute intervals.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is entered, all access list log information managed by access list logging is cleared.

Related commands

access-log enable

access-log rate-limit

Specifies the maximum number of packets transferred to the CPU per second for BSU, CSU, or MSU. Any packets exceeding the upper limit value are discarded.

Syntax

To set information:

access-log rate-limit <*number*>

To delete information:

no access-log rate-limit

Input mode

`(config)`

Parameters

<*number*>

Specifies the maximum number of packets transferred to the CPU per second. If 0 is specified, no packets are transferred.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0, or 10 to 250

Default behavior

The maximum number of packets transferred to the CPU per second is 100.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The value specified by this command is the maximum number of packets transferred to the CPU per second. Transmission of the specified number of packets, however, is not guaranteed.

Related commands

access-log enable

access-log threshold

Outputs an access list log at the time the number of packets reaches N (1 or larger) times the specified threshold value.

Syntax

To set information:

access-log threshold <*packet count*>

To delete information:

no access-log threshold

Input mode

`(config)`

Parameters

<*packet count*>

Specifies the number of packets that trigger the output of an access list log.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4294967295

Default behavior

Access list log output is not triggered based on a threshold value.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. An access list log is output when the first packet in a flow is received. After that, the access list log output repeats each time the number of packets in the flow reaches N (1 or larger) times the specified threshold value.
2. If a small value is specified for the threshold value and a large number of packets are subject to access list logging, many access list log files might be output in a short time. If this happens, some of the access list logs might not be able to output due to CPU overload.

Related commands

access-log enable

Chapter 6. uRPF

ip urpf
ip verify unicast source reachable-via
ipv6 verify unicast source reachable-via

ip urpf

Enables the uRPF functionality.

Syntax

To set information:

ip urpf [allow-default]

To delete information:

no ip urpf

Input mode

(config)

Parameters

allow-default

Specifies that the default route be subject to uRPF checking.

This setting is valid for both Strict and Loose modes on all interfaces.

1. Default value when this parameter is omitted:

   The default route is not subject to uRPF checking.

2. Range of values:

   None

Default behavior

The uRPF functionality cannot be used. Use the `ip urpf` command to enable the uRPF functionality.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting also takes effect for IPv6.
2. This command cannot enable uRPF functionality if the number of multipaths is set to 9 or more in the `maximum-paths` command. Change the number of multipaths to no more than 8 before using this command.

   If the number of multipaths is changed from 9 or more to no more than 8, it will take a certain period of time until the route information is applied to the hardware. During this period, uRPF might not function properly. Therefore, if you change the number of multipaths from 9 or more to no more than 8, we recommend that you restart the switch before setting this command.

Related commands

ip verify unicast source reachable-via

ipv6 verify unicast source reachable-via

ip route static maximum-paths

maximum-paths (OSPF)

maximum-paths (BGP4)

ipv6 route static maximum-paths

maximum-paths (OSPFv3)

maximum-paths (BGP4+)

ip verify unicast source reachable-via

Enables uRPF for IPv4.

Syntax

To set information:

ip verify unicast source reachable-via { rx | any }

To delete information:

no ip verify unicast source reachable-via

Input mode

(config-if)

Parameters

{ rx | any }

Sets the uRPF operating mode.

rx

Strict mode

any

Loose mode

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

uRPF for IPv4 is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is valid only if the `ip urpf` command is set.
2. If the `ipv6 verify unicast source reachable-via` command has already been set on the same interface, you cannot change the operating mode.

Related commands

ip urpf

ipv6 verify unicast source reachable-via

ipv6 verify unicast source reachable-via

Enables uRPF for IPv6.

Syntax

To set information:

ipv6 verify unicast source reachable-via { rx | any }

To delete information:

no ipv6 verify unicast source reachable-via

Input mode

`(config-if)`

Parameters

{ rx | any }

Sets the uRPF operating mode.

rx

Strict mode

any

Loose mode

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

uRPF for IPv6 is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is valid only if the `ip urpf` command is set.
2. If the `ip verify unicast source reachable-via` command has already been set on the same interface, you cannot change the operating mode.

Related commands

ip urpf

ip verify unicast source reachable-via

Chapter 7. QoS

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
llrlq1-burst [AX6700S] [AX6600S]
llrlq2-burst [AX6700S] [AX6600S]
mac qos-flow-group
mac qos-flow-list
mac qos-flow-list resequence
mode
number-of-queue
predicted-tail-drop
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
set-default-user-priority
shaper auto-configuration
shaper default-user
shaper llrlq1 [AX6700S] [AX6600S]
shaper llrlq2 [AX6700S] [AX6600S]
shaper nif
shaper port buffer
shaper port rate-limit
shaper user
shaper user-list
shaper vlan-user-map
shaper wgq-group rate-limit [AX6700S] [AX6600S]
traffic-shape rate
upc-storm-control mode

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 7-1: 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 7-2: 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 7-3: 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 7-4: 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 7-5: 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 name

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

Table 7-6: 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 name

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

Table 7-7: 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 name

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

Table 7-8: 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 name

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

Table 7-9: Ethernet type names that can be specified

Ethernet type name	Ethernet value	Remarks
appletalk	0x809b	
arp	0x0806	
axp	0x88f3	Alaxala Protocol
eapol	0x888e	
gsrp	--#	Performs flow detection for 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 7-10: Destination MAC address names that can be specified

Destination address specification	Destination address	Destination address mask
bpdu	0180.C200.0000	0000.0000.0000
cdp	0100.0CCC.CCCC	0000.0000.0000
lacp	0180.C200.0002	0000.0000.0000
lldp	0100.8758.1310	0000.0000.0000
oadp	0100.4C79.FD1B	0000.0000.0000
pvst-plus-bpdu	0100.0CCC.CCCD	0000.0000.0000

Destination address specification	Destination address	Destination address mask
slow-protocol	0180.C200.0002	0000.0000.0000

Message name (ICMP)

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

Table 7-11: 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
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4

Message name	Message	Type	Code
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 7-12: 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
packet-too-big	Packet too big	2	Not specified
parameter-option	Parameter option problems	4	2

Message name	Message	Type	Code
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

Range of values specifiable for bandwidth monitoring

The following table lists the range of values specifiable for bandwidth monitoring.

Table 7-13: Message names that can be specified for ICMP (IPv6)

Setting range		Increment
In Gbit/s	1 G to 10 G	1 G#
In Mbit/s	1 M to 10000 M	1 M#
In kbit/s	5 to 10000000	--

Legend: --: Not applicable

#: 1 G = 1000000 k. 1 M = 1000 k.

Number of QoS flow lists that can be created

The number of QoS flow lists that can be created is the number of names that can be used as QoS flow list IDs. The maximum number of lists that can be created for <*qos flow list name*> of the corresponding configuration is shown below.

- For AX6700S series switches:

  The following table lists the number of QoS flow lists that can be created for each BSU type.

  Table 7-14: Number of QoS flow lists that can be created for each BSU type

BSU type	QoS flow list	Flow detection and action specifications
All models	8574 lists	32000 entries#

  #: Filter condition entries in access lists are included.

- For AX6600S series switches:

  The number of QoS flow lists, flow detection conditions, and action specification entries that can be created per device depends on the CSU type. The following table lists the number of QoS flow lists that can be created for each CSU type.

Table 7-15: Number of QoS flow lists that can be created for each CSU type

CSU type	QoS flow list	Flow detection and action specifications
CSU-1A	4000 lists	4000 entries
CSU-1B	8574 lists	32000 entries#

#: Filter condition entries in access lists are included.

- For AX6300S series switches:

  The number of QoS flow lists, flow detection conditions, and action specification entries that can be created per device depends on the MSU type. The following table lists the number of QoS flow lists that can be created for each MSU type.

Table 7-16: Number of QoS flow lists that can be created for each MSU type

MSU type	QoS flow list	Flow detection and action specifications
MSU-1A and MSU-1A1	4000 lists	4000 entries
MSU-1B and MSU-1B1	8574 lists	32000 entries#

#: Filter condition entries in access lists are included.

Number of specifications that can be set for an interface

The number of specifications that can be set for an interface is the total number of QoS flow lists that can be set for an interface. The maximum number of lists that can be created is shown below.

Specifications are counted separately for the receiving side, sending side, and the forwarding type. 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. Similarly, if both Layer 2 forwarding and Layer 3 forwarding are set for the same interface, it is counted as two lists.

- For AX6700S series switches:

  The following table lists the number of specifications that can be set for an interface for each BSU type.

Table 7-17: Number of specifications that can be set for an interface for each BSU type

BSU type	Number of specifications that can be set
All models	8574 lists

- For AX6600S series switches:

  The number of `ip qos-flow-group`, `ipv6 qos-flow-group`, `mac qos-flow-group`, and `advance qos-flow-group` settings available for a Switch depends on the CSU type. The following table lists the number of specifications that can be set for an interface for each CSU type.

Table 7-18: Number of specifications that can be set for an interface for each CSU type

CSU type	Number of specifications that can be set
CSU-1A	4000 lists
CSU-1B	8574 lists

■ For AX6300S series switches:

The number of `ip qos-flow-group`, `ipv6 qos-flow-group`, `mac qos-flow-group`, and `advance qos-flow-group` settings available for a Switch depends on the MSU type. The following table lists the number of specifications that can be set for an interface for each MSU type.

Table 7-19: Number of specifications that can be set for an interface for each MSU type

MSU type	Number of specifications that can be set
MSU-1A and MSU-1A1	4000 lists
MSU-1B and MSU-1B1	8574 lists

Examples of calculating the number of QoS flow lists that can be created and the number of specifications that can be set for an interface

The following table provides examples of calculating the number of QoS flow lists that can be created and the number of specifications that can be set for an interface.

Table 7-20: Examples for calculating the number of QoS flow lists that can be created and the number of specifications that can be set for an interface

Sample code	Number of QoS flow lists created	Number of specifications set for the interface

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 layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action min-rate 10M`
	1 list	1 list

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 layer2-forwarding`
 	
`interface gigabitethernet 2/2`
`ip qos-flow-group AAA in layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action min-rate 10M`
	1 list	2 lists

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 layer2-forwarding`
`ip qos-flow-group AAA out layer2-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action max-rate 10M`
	1 list	2 lists

In this example, QoS flow list `AAA` is created and `layer2-forwarding` and `layer3-forwarding` are set for `inbound` on the VLAN 2 interface.
`interface vlan 2`
`ip qos-flow-group AAA in layer2-forwarding`
`ip qos-flow-group AAA in layer3-forwarding`
 	
`ip qos-flow-list AAA`
`10 qos tcp any any action max-rate 10M`
`20 qos udp any any action max-rate 10M`
	1 list	2 lists

Sample code	Number of QoS flow lists created	Number of specifications set for the interface

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 layer2-forwarding`
 	
`interface gigabitethernet 2/2`
`  ip qos-flow-group BBB in layer2-forwarding`
 	
`ip qos-flow-list AAA`
`  10 qos tcp any any action max-rate 10M`
`  20 qos udp any any action max-rate 10M`
 	
`ip qos-flow-list BBB`
`  10 qos udp any any action max-rate 10M`
`  20 qos tcp any any action min-rate 10M`
	2 lists	2 lists

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 layer2-forwarding`
`  ip qos-flow-group BBB out layer2-forwarding`
 	
`ip qos-flow-list AAA`
`  10 qos tcp any any action max-rate 10M`
`  20 qos udp any any action max-rate 10M`
 	
`ip qos-flow-list BBB`
`  10 qos udp any any action max-rate 10M`
`  20 qos tcp any any action min-rate 10M`
	2 lists	2 lists

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 max-rate 10M`
	1 list	0 lists

advance qos-flow-group

Enables the QoS functionality by applying an Advance QoS flow list to an Ethernet interface or a VLAN interface.

For details about the number of specifications that can be set for an interface, see *Number of specifications that can be set for an interface*.

Syntax

To set information:

- Ethernet interface

  advance qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

- VLAN interface

  advance qos-flow-group <*qos flow list name*> {in | out} layer2-and-layer3-forwarding

To delete information:

- Ethernet interface

  no advance qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

- VLAN interface

  no advance qos-flow-group <*qos flow list name*> {in | out} layer2-and-layer3-forwarding

Input mode

`(config-if)`

Parameters

<*qos flow list name*>

Specify the name of an Advance QoS flow list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects packets forwarded on Layer 2 in flow detection.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

layer2-and-layer3-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-and-layer3-forwarding` detects packets forwarded on Layer 2 and Layer 3 in flow detection.

This parameter has an effect only when it is applied to a VLAN interface.

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. On an interface, you can set one Advance QoS flow list for each of Inbound and Outbound.

   If an Advance QoS flow list has already been set, first remove it and then set it again.

2. If you specify a non-existent Advance QoS flow list, this will be ignored. The identifier of the Advance QoS flow list is registered.

3. You can set an Advance QoS flow list if the flow distribution pattern is `default standard-advance`, `default extended-advance`, `qos-only extended-advance`, `filter extended-advance`, or `qos extended-advance`.

4. When `mac-ip` is specified for the flow detection condition type and the `own-address` or `own` parameter is specified in the flow detection condition, you can set an Advance QoS flow list if an IPv4 address is set for the target interface.

5. When `mac-ipv6` is specified for the flow detection condition type and the `own-address` parameter is specified in the flow detection condition, you can set an Advance QoS flow list if one IPv6 global address only is set for the target interface.

6. When an Advance QoS flow list is to be applied to an Ethernet interface and a VLAN parameter is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.

7. When an Advance QoS flow list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.

8. Bandwidth monitoring can be set so that both maximum bandwidth control and minimum

bandwidth monitoring are set for the flow detection condition if `upc-in-in` is set for bandwidth monitoring storm control mode for Inbound.

9. Bandwidth monitoring can be set for Inbound of an Ethernet interface only. [AX6700S]
10. Bandwidth monitoring can also be set for Outbound if `upc-in-out` is set for bandwidth monitoring storm control mode. [AX6600S] [AX6300S]
11. When you set bandwidth monitoring for Inbound of a VLAN interface, specify 1 for the number of running PSP units in the following commands. [AX6600S]
    - redundancy max-psp
    - schedule-power-control max-psp
    - adaptive-power-control max-psp

Related commands

advance qos-flow-list

advance qos-flow-list

Creates an Advance QoS flow list to be used to set QoS flow detection and action specifications.

For details of the number of QoS flow lists, flow detection conditions, and action specification entries that can be created for a Switch, see *Number of QoS flow lists that can be created*.

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*>

Specify the name of an Advance QoS flow list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

1. You cannot specify IPv4 QoS flow list names, IPv6 QoS flow list names, and MAC QoS flow list names that have already been created.

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 name of the Advance QoS flow list to be changed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

Enables the QoS functionality by applying an IPv4 QoS flow list to an Ethernet interface or a VLAN interface.

For details about the number of specifications that can be set for an interface, see *Number of specifications that can be set for an interface*.

Syntax

To set information:

- Ethernet interface

  ip qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

- VLAN interface

  ip qos-flow-group <*qos flow list name*> {in | out} {layer2-forwarding | layer3-forwarding}

To delete information:

- Ethernet interface

  no ip qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

- VLAN interface

  no ip qos-flow-group <*qos flow list name*> {in | out} {layer2-forwarding | layer3-forwarding}

Input mode

```
(config-if)
```

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 name that is no more than 31 characters long.

   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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{layer2-forwarding | layer3-forwarding}

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

`layer3-forwarding` detects IP packets forwarded on Layer 3 in flow detection.

This parameter has an effect only when it is applied to a VLAN interface.

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. On an Ethernet interface, you can set one IPv4 QoS flow list for each of Inbound and Outbound.

   On a VLAN interface, you can set one IPv4 QoS flow list for each of Inbound Layer 2 forwarding, Inbound Layer 3 forwarding, Outbound Layer 2 forwarding, and Outbound Layer 3 forwarding.

   If an IPv4 QoS flow list has already been set, first remove it and then set it again.

2. If you specify a non-existent IPv4 QoS flow list name, this will be ignored. The IPv4 QoS flow list name is registered.

3. You can set an IPv4 QoS flow list if the flow distribution pattern is `default standard`, `default standard-advance`, `default extended`, `default extended-advance`, `qos-only extended`, `qos-only extended-advance`, `filter extended`, `filter extended-advance`, `qos extended`, or `qos extended-advance`.

4. When the `own-address` or `own` parameter is specified in the flow detection condition, you can set an IPv4 QoS flow list if an IPv4 address is set for the target interface.

5. When an IPv4 QoS flow list is to be applied to the Layer 2 forwarding of an Ethernet or VLAN interface, you can set the list if MAC mode is not set.

6. When an IPv4 QoS flow list is to be applied to an Ethernet interface and a VLAN parameter is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.

7. When an IPv4 QoS flow list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.
8. When an IPv4 QoS flow list is to be applied to Layer 2 forwarding of an Ethernet or VLAN interface, you can set the list if neither `tcp` flag nor `tos` parameter is set in the flow detection condition and neither the parameter for DSCP updating nor the parameter for DSCP updating at minimum bandwidth non-compliance is set for action.
9. Bandwidth monitoring can be set so that both maximum bandwidth control and minimum bandwidth monitoring are set for the flow detection condition if `upc-in-in` is set for bandwidth monitoring storm control mode for Inbound.
10. Bandwidth monitoring can be set for Inbound of an Ethernet interface only. [AX6700S]
11. Bandwidth monitoring can also be set for Outbound if `upc-in-out` is set for bandwidth monitoring storm control mode. [AX6600S] [AX6300S]
12. When you set bandwidth monitoring for Inbound of a VLAN interface, specify 1 for the number of running PSP units in the following commands. [AX6600S]
    - redundancy max-psp
    - schedule-power-control max-psp
    - adaptive-power-control max-psp

Related commands

ip qos-flow-list

ip qos-flow-list

Creates an IPv4 QoS flow list to be used to set QoS flow detection and action specifications.

For details of the number of QoS flow lists, flow detection conditions, and action specification entries that can be created for a Switch, see *Number of QoS flow lists that can be created*.

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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

1. You cannot specify IPv6 QoS flow list names, MAC QoS flow list names, and Advance QoS flow list names that have already been created.

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 name of the IPv4 QoS flow list to be changed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

Enables the QoS functionality by applying an IPv6 QoS flow list to an Ethernet interface or a VLAN interface.

For details about the number of specifications that can be set for an interface, see *Number of specifications that can be set for an interface*.

Syntax

To set information:

- Ethernet interface

  ipv6 qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

- VLAN interface

  ipv6 qos-flow-group <*qos flow list name*> {in | out} {layer2-forwarding | layer3-forwarding}

To delete information:

- Ethernet interface

  no ipv6 qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

- VLAN interface

  no ipv6 qos-flow-group <*qos flow list name*> {in | out} {layer2-forwarding | layer3-forwarding}

Input mode

`(config-if)`

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 name that is no more than 31 characters long.

   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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{layer2-forwarding | layer3-forwarding}

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects IP packets forwarded on Layer 2 in flow detection.

`layer3-forwarding` detects IP packets forwarded on Layer 3 in flow detection.

This parameter has an effect only when it is applied to a VLAN interface.

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. On an Ethernet interface, you can set one IPv6 QoS flow list for each of Inbound and Outbound.

   On a VLAN interface, you can set one IPv6 QoS flow list for each of Inbound Layer 2 forwarding, Inbound Layer 3 forwarding, Outbound Layer 2 forwarding, and Outbound Layer 3 forwarding.

   If an IPv6 QoS flow list has already been set, first remove it and then set it again.

2. If you specify a non-existent IPv6 QoS flow list name, this will be ignored. The IPv6 QoS flow list name is registered.

3. You can set an IPv6 QoS flow list if the flow distribution pattern is `default standard`, `default standard-advance`, `default extended`, `default extended-advance`, `qos-only extended`, `qos-only extended-advance`, `filter extended`, `filter extended-advance`, `qos extended`, or `qos extended-advance`.

4. When the `own-address` parameter is specified in the flow detection condition, you can set an IPv6 QoS flow list if one IPv6 global address only is set for the target interface.

5. You can set an IPv6 QoS flow list if, for the source address which is a parameter in the flow detection condition, `any` is specified or a value no more than 64 is specified for `Len`.

6. When an IPv6 QoS flow list is to be applied to the Layer 2 forwarding of an Ethernet or VLAN interface, you can set the list if MAC mode is not set.

7. When an IPv6 QoS flow list is to be applied to an Ethernet interface and a VLAN parameter

is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.

8. When an IPv6 QoS flow list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.
9. When an IPv6 QoS flow list is to be applied to Layer 2 forwarding of an Ethernet or VLAN interface, you can set the list if neither `tcp` flag nor `traffic-class` parameter is set in the flow detection condition and neither the parameter for DSCP updating nor the parameter for DSCP updating at minimum bandwidth non-compliance is set for action.
10. Bandwidth monitoring can be set so that both maximum bandwidth control and minimum bandwidth monitoring are set for the flow detection condition if `upc-in-in` is set for bandwidth monitoring storm control mode for Inbound.
11. Bandwidth monitoring can be set for Inbound of an Ethernet interface only. [AX6700S]
12. Bandwidth monitoring can also be set for Outbound if `upc-in-out` is set for bandwidth monitoring storm control mode. [AX6600S] [AX6300S]
13. When you set bandwidth monitoring for Inbound of a VLAN interface, specify 1 for the number of running PSP units in the following commands. [AX6600S]
    - redundancy max-psp
    - schedule-power-control max-psp
    - adaptive-power-control max-psp

Related commands

ipv6 qos-flow-list

ipv6 qos-flow-list

Creates an IPv6 QoS flow list to be used to set QoS flow detection and action specifications.

For details of the number of QoS flow lists, flow detection conditions, and action specification entries that can be created for a Switch, see *Number of QoS flow lists that can be created*.

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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

1. You cannot specify IPv4 QoS flow list names, MAC QoS flow list names, and Advance QoS flow list names that have already been created.

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 name of the IPv6 QoS flow list to be changed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

llrlq1-burst [AX6700S] [AX6600S]

Applicable shaper modes

[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

Specifies the burst size for LLRLQ1.

For LLRLQ1 for the specified NIF, the standard send bandwidth and burst size are set.

For LLRLQ1 for each interface of the NIF, the burst size calculated from the following formula is set:

<send bandwidth for this parameter> : *<burst size for this parameter>* =

<maximum bandwidth for each LLRLQ1> : *<burst size for each LLRLQ1>*

Syntax

To set or change information:

llrlq1-burst <*Mbit/s*>M <*byte*>

To delete information:

no llrlq1-burst

Input mode

```
(config-sh-nif)
```

Parameters

<*Mbit/s*>M

Specifies the standard send bandwidth.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 1000.

<*byte*>

Specifies the standard burst size.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 32000.

Default behavior

The burst size is not set for LLRLQ1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When you use this command, specify the maximum bandwidth value from 1 M to 100 M for the user list set for `llrlq1`.

Related commands

None

llrlq2-burst [AX6700S] [AX6600S]

Applicable shaper mode

[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

Specifies the burst size for LLRLQ2.

For LLRLQ2 for the specified NIF, the standard send bandwidth and burst size are set.

For LLRLQ2 for each interface of the NIF, the burst size calculated from the following formula is set:

<send bandwidth for this parameter> : *<burst size for this parameter>* =

<maximum bandwidth for each LLRLQ2> : *<burst size for each LLRLQ2>*

Syntax

To set or change information:

llrlq2-burst <*Mbit/s*>M <*byte*>

To delete information:

no llrlq2-burst

Input mode

```
(config-sh-nif)
```

Parameters

<*Mbit/s*>M

Specifies the standard send bandwidth.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 1000.

<*byte*>

Specifies the standard burst size.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 32000.

Default behavior

The burst size is not set for LLRLQ2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When you use this command, specify the maximum bandwidth value from 1 M to 100 M for the user list set for `llrlq2`.

Related commands

None

mac qos-flow-group

Enables the QoS functionality by applying a MAC QoS flow list to an Ethernet interface or a VLAN interface.

For details about the number of specifications that can be set for an interface, see *Number of specifications that can be set for an interface*.

Syntax

To set information:

mac qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

To delete information:

no mac qos-flow-group <*qos flow list name*> {in | out} layer2-forwarding

Input mode

`(config-if)`

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 name that is no more than 31 characters long.

   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

layer2-forwarding

Specifies the forwarding type to be detected in flow detection.

`layer2-forwarding` detects packets forwarded on Layer 2 in flow detection.

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. On an interface, you can set one MAC QoS flow list for each of Inbound and Outbound. If a MAC QoS flow list has already been set, first remove it and then set it again.
2. If you specify a non-existent MAC QoS flow list, this will be ignored. The identifier of the MAC QoS flow list is registered.
3. You can set a MAC QoS flow list if the flow distribution pattern is `default standard`, `default standard-advance`, `default extended`, `default extended-advance`, `qos-only extended`, `qos-only extended-advance`, `filter extended`, `filter extended-advance`, `qos extended`, or `qos extended-advance`.
4. When a MAC QoS flow list is to be applied to an Ethernet interface and a VLAN parameter is set in the flow detection condition, you can set the list if all VLAN IDs corresponding to the VLAN parameters are included in the settings of the Ethernet interface.
5. When a MAC QoS flow list is to be applied to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection condition.
6. Bandwidth monitoring can be set so that both maximum bandwidth control and minimum bandwidth monitoring are set for the flow detection condition if `upc-in-in` is set for bandwidth monitoring storm control mode for Inbound.
7. Bandwidth monitoring can be set for Inbound of an Ethernet interface only. [AX6700S]
8. Bandwidth monitoring can also be set for Outbound if `upc-in-out` is set for bandwidth monitoring storm control mode. [AX6600S] [AX6300S]
9. When you set bandwidth monitoring for Inbound of a VLAN interface, specify 1 for the number of running PSP units in the following commands. [AX6600S]
   - redundancy max-psp
   - schedule-power-control max-psp
   - adaptive-power-control max-psp

Related commands

mac qos-flow-list

mac qos-flow-list

Creates a MAC QoS flow list used to set QoS flow detection and action specifications.

For details of the number of QoS flow lists, flow detection conditions, and action specification entries that can be created for a Switch, see *Number of QoS flow lists that can be created*.

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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

1. You cannot specify IPv4 QoS flow list names, IPv6 QoS flow list names, and Advance QoS flow list names that have already been created.

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 to be changed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   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

mode

Configures shaper mode. This command is used to determine the bandwidth control method for a hierarchical shaper for the target NIF. The shaper mode setting cannot be changed if a shaper configuration is set for the NIF for which this command is to be set. This command cannot be set if the shaper auto setting functionality is used.

Syntax

To set or change information:

mode { rgq | wgq | llpq1 | llpq2 | llpq4 }[llrlq] [AX6700S] [AX6600S]

To set information:

mode rgq [AX6300S]

To delete information:

no mode

Input mode

```
(config-sh-nif)
```

Parameters

{ rgq | wgq | llpq1 | llpq2 | llpq4 } [AX6700S] [AX6600S]

rgq

Sets the bandwidth control method to RGQ. The RGQ method guarantees a minimum bandwidth for each user. Users will have the same output priority.

wgq

Sets the bandwidth control method to WGQ. The WGQ method allocates bandwidth based on the ratio of the weight for each user. Users will have the same output priority.

llpq1

Sets shaper mode to LLPQ1 and the bandwidth control method to LLPQ. The LLPQ1 method allows each user to have one queue with low delay, and guarantees a minimum bandwidth for each user. The output priority of a queue with low delay will be higher than that of a normal queue for all users. Users will have the same output priority.

llpq2

Sets shaper mode to LLPQ2 and the bandwidth control method to LLPQ. The LLPQ2 method allows each user to have two queues with low delay, and guarantees a minimum bandwidth for each user. The output priority of a queue with low delay will be higher than that of a normal queue for all users. Users will have the same output priority.

llpq4

Sets shaper mode to LLPQ4 and the bandwidth control method to LLPQ. The LLPQ4 method allows each user to have four queues with low delay, and guarantees a minimum bandwidth for each user. The output priority of a queue with low delay will be higher than that of a normal queue for all users. Users will have the same output priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify rgq, wgq, llpq1, llpq2, or llpq4.

3. Note on using this parameter:

   If the `llpq1` parameter is specified and the number of queues is four, the fourth queue becomes the queue with low delay. If the number of queues is eight, the eighth queue becomes the queue with low delay.

   If the `llpq2` parameter is specified and the number of queues is four, the third and fourth queues become the queues with low delay. If the number of queues is eight, the seventh and eighth queues become the queues with low delay.

   If the `llpq4` parameter is specified and the number of queues is eight, the queues from the fifth to eighth become the queues with low delay. You cannot select 4 for the number of queues.

llrlq [AX6700S] [AX6600S]

Enables the setting of the two low-delay high-priority users (llrlq1 and llrlq2), which are independent from the users specified in shaper mode. The output priority is as follows:

llrlq1 > llrlq2 > all users

1. Default value when this parameter is omitted:

   llrlq1 and llrlq2 cannot be set.

2. Range of values:

   None

3. Note on using this parameter:

   If this parameter is set, the number of users that can be used in the specified shaper mode will be reduced by two.

rgq [AX6300S]

Sets the bandwidth control method to RGQ. The RGQ method guarantees a minimum bandwidth for each user. Users will have the same output priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `rgq`.

Default behavior

Shaper mode is not configured.

Impact on communication

When the setting is changed or deleted, the NIF is reset and communication is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For a receiving-side interface (Ethernet or VLAN) of the device, if a QoS flow list is set and a user of the hierarchical shaper functionality, llrlq1, or llrlq2 is specified in the action parameter for that QoS flow list, note the following conditions: [AX6700S] [AX6600S]

   - When configuring shaper mode, make sure that all the settings for shaper mode and the number of queues are the same on the NIF for which shaper mode has been set.
   - You cannot change shaper mode.

- You cannot delete all shaper mode settings that have already been set. At least one setting must remain on the device.

2. For a receiving-side interface (Ethernet or VLAN) of the device, if a QoS flow list is specified and a user of the hierarchical shaper functionality is specified in the action parameter for that QoS flow list, note the following conditions: [AX6300S]
   - When configuring shaper mode, make sure that all the settings for the number of queues are the same on the NIF for which shaper mode has been set.
   - You cannot delete all shaper mode settings that have already been set. At least one setting must remain on the device.
3. For a sending-side interface (Ethernet) of the target NIF, if a QoS flow list is set and a user of the hierarchical shaper functionality, llrlq1, or llrlq2 is specified in the action parameter for that QoS flow list, shaper mode cannot be changed or deleted. [AX6700S] [AX6600S]
4. For a sending-side interface (Ethernet) of the target NIF, if a QoS flow list is specified and a user of the hierarchical shaper functionality is specified in the action parameter for that QoS flow list, shaper mode cannot be deleted. [AX6300S]
5. For a sending-side interface (VLAN) to which ports on the target NIF belong, if a QoS flow list is set and a user of the hierarchical shaper functionality, llrlq1, or llrlq2 is specified in the action parameter for that QoS flow list, note the following conditions: [AX6700S] [AX6600S]
   - When configuring shaper mode, make sure that all the settings for shaper mode and the number of queues are the same on the NIF that has ports belonging to the target VLAN and on which shaper mode has been set.
   - You cannot change the shaper mode setting set for a NIF that has ports belonging to the target VLAN.
   - You cannot delete a shaper mode setting if doing so causes no shaper mode settings to remain for all NIFs that have ports belonging to the target VLAN.
6. For a sending-side interface (VLAN) to which ports on the target NIF belong, if a QoS flow list is specified and a user of the hierarchical shaper functionality is specified in the action parameter for that QoS flow list, note the following conditions: [AX6300S]
   - When configuring shaper mode, make sure that all the settings for the number of queues are the same on all the NIFs that have ports belonging to the target VLAN and on which shaper mode has been set.
   - You cannot delete a shaper mode setting if doing so causes no shaper mode settings to remain for all NIFs that have ports belonging to the target VLAN.

Related commands

None

number-of-queue

Applicable shaper modes

[rgq] [rgq llrlq] [wgq] [wgq llrlq] [llpq1] [llpq1 llrlq] [llpq2] [llpq2 llrlq]

Sets the number of queues allowed for a user for the specified shaper NIF. Information cannot be set or deleted if shaper configuration has been set for the interface of the NIF for which this command is to be set.

Syntax

To set information:

number-of-queue 4

To delete information:

no number-of-queue

Input mode

(config-sh-nif)

Parameters

4

Specifies 4 as the number of queues allowed for a user.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The number of queues allowed for a user is set to 8.

Impact on communication

When the setting is changed or deleted, the NIF is reset and communication is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a NIF to which shaper mode has not been applied.
2. For a receiving-side interface (Ethernet or VLAN) of the device, if a QoS flow list is set and a user of the hierarchical shaper functionality, llrlq1, or llrlq2 is specified in the action parameter for that QoS flow list, you cannot change the number of queues for the NIF for which shaper mode has been set. [AX6700S] [AX6600S]
3. For a receiving-side interface (Ethernet or VLAN) of the device, if a QoS flow list is specified and a user of the hierarchical shaper functionality is specified in the action parameter for that QoS flow list, you cannot change the number of queues for the NIF for which shaper mode has been set. [AX6300S]
4. For a sending-side interface (Ethernet) of the target NIF, if a QoS flow list is set and a user of the hierarchical shaper functionality, llrlq1, or llrlq2 is specified in the action parameter for that QoS flow list, you cannot change the number of queues for the NIF for which shaper

mode has been set. [AX6700S] [AX6600S]

5. For a sending-side interface (Ethernet) of the target NIF, if a QoS flow list is specified and a user of the hierarchical shaper functionality is specified in the action parameter for that QoS flow list, you cannot change the number of queues for the NIF for which shaper mode has been set. [AX6300S]
6. For a sending-side interface (VLAN) to which the ports on the target NIF belong, if a QoS flow list is set and a user of the hierarchical shaper functionality, llrlq1, or llrlq2 is specified in the action parameter for that QoS flow list, you cannot change the number of queues for the NIF that has the ports belonging to the target VLAN and for which shaper mode has been set. [AX6700S] [AX6600S]
7. For a sending-side interface (VLAN) to which the ports on the target NIF belong, if a QoS flow list is specified and a user of the hierarchical shaper functionality is specified in the action parameter for that QoS flow list, you cannot change the number of queues for the NIF that has the ports belonging to the target VLAN and for which shaper mode has been set. [AX6300S]

Related commands

shaper nif

predicted-tail-drop

Applicable shaper modes

All shaper modes

Disables the predicted tail drop functionality for the specified NIF or for all NIFs on the device.

If the QoS buffer assigned to a port is 7/8 full, this functionality halves the length of the queue that has the same queue number as the full QoS number, for all users set for the interface of that port.

Syntax

To set information:

predicted-tail-drop disable

To delete information:

no predicted-tail-drop

Input mode

```
(config-sh-nif)
```

Parameters

None

Default behavior

The predicted tail drop functionality is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

shaper nif

qos (advance qos-flow-list)

Specifies flow detection conditions and action specifications in the Advance QoS flow list.

Syntax

To set or change information:

[<*sequence*>] qos mac {flow detection condition}[action specification]

[<*sequence*>] qos mac-ip {flow detection condition}[action specification]

[<*sequence*>] qos mac-ipv6 {flow detection condition}[action specification]

- For `mac {`flow detection condition`}`:

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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} [<*ethernet type*>][vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- For `mac-ip {`flow detection condition`}`:

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

When "packet is not fragmented" is a condition, and the upper-layer protocol is 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ip | <*protocol*>} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} tcp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When "packet is not fragmented" is a condition, 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} igmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [<*igmp type*>] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When "packet is fragmented" is a condition

mac-ip {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [fragments] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- For `mac-ipv6 {`flow detection condition`}`:

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

When the upper-layer protocol is 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} {ipv6 | <*protocol*>} {<*source ipv6*>/<*length*>|

host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*source ipv6 start*> <*source ipv6 end*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} tcp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | 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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} udp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

When 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 | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} icmp {<*source ipv6*>/<*length*>| host {<*source ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*source ipv6 start*> <*source ipv6 end*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>][{ctag-untagged | [ctag-user-priority <*priority*>] [ctag-vlan <*vlan id*>]}]

- Action specification

When DSCP mapping is not to be used

action [user <*user id*> | llrlq1 | llrlq2] [priority-class <*class*>] [discard-class <*class*>] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>] [max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>] [min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>] [penalty-discard-class <*class*>] [penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

When DSCP mapping is to be used

action [user <*user id*> | llrlq1 | llrlq2] [dscp-map] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>] [max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>] [min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>] [penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

To delete information:

no <*sequence*>

Input mode

`(config-adv-qos)`

Parameters

<*sequence*>

Sets the application sequence in the QoS flow list to be created or changed.

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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the source MAC address.

To specify all source MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source mac*> <*source mac mask*>, `host` <*source mac*>, or `any`.

   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.

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

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

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

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol}

Specifies the destination MAC address.

To specify all destination MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination mac*> <*destination mac mask*>, `host` <*destination mac*>, `any`, `bpdu`, `cdp`, `lacp`, `lldp`, `oadp`, `pvst-plus-bpdu`, or `slow-protocol`.

   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.

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

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

   If `bpdu` is specified, BPDU control packets are used as the flow detection condition.

   If `cdp` is specified, CDP control packets are used as the flow detection condition.

   If `lacp` or `slow-protocol` is specified, slow protocol packets are used as the flow detection condition.

   This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD functionality.

   If `lacp` is specified, LACP control packets are used as the flow detection condition.

   If `lldp` is specified, LLDP control packets are used as the flow detection condition.

   If `oadp` is specified, OADP control packets are used as the flow detection condition.

   If `pvst-plus-bpdu` is specified, PVST+ control packets are used as the flow detection condition.

   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 protocol names that can be specified, see *Table 7-9: Ethernet type names that can be specified*.

vlan {<*vlan id*> | <*vlan id list name*>}

Specifies the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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.

ctag-untagged

Specifies detection of packets with no customer tag.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

ctag-user-priority <*priority*>

Specifies a user priority for the customer 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.

ctag-vlan <*vlan id*>

Specifies a VLAN ID for the customer 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 7-1: 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 7-2: Protocol names that can be specified (IPv6)*.

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

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv4*> <*source ipv4 wildcard*>, `host` <*source ipv4*>, `any`, `own-address` <*source ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*source ipv4 start*> <*source ipv4 end*>.

   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.

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

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

   `own-address` and `own` are valid only for a VLAN interface.

   If `own-address` is specified, the flow detection condition is the source IPv4 address that has been set on the target interface.

   If `own` is specified, the flow detection condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the flow detection condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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 | range-address <*source ipv6 start*> <*source ipv6 end*>}

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv6*>/<*length*>, `own-address` <*own address length*>, `host` <*source ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*source ipv6 start*> <*source ipv6 end*>.

   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.

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

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

`own-address` and `own` are valid only for a VLAN interface.

If `own-address` is specified, the flow detection condition is the source IPv6 address that has been set as the IPv6 global address on the target interface.

If `own` is specified, the flow detection conditions are the source IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

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.

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 7-3: Port names that can be specified for TCP*, *Table 7-4: Port names that can be specified for UDP (IPv4)*, and *Table 7-5: Port names that can be specified for UDP (IPv6)*.

   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*>.

   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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv4*> <*destination ipv4 wildcard*>, `host` <*destination ipv4*>, `any`, `own-address` <*destination ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*destination ipv4 start*> <*destination ipv4 end*>.

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.

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

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

`own-address` and `own` are valid only for a VLAN interface.

If `own-address` is specified, the flow detection condition is the destination IPv4 address that has been set on the target interface.

If `own` is specified, the flow detection condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the flow detection condition is assumed to be arbitrary.

If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv6*>/<*length*>, `own-address` <*own address length*>, `host` <*destination ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*destination ipv6 start*> <*destination ipv6 end*>.

   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 `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

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

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

   `own-address` and `own` are valid only for a VLAN interface.

   If `own-address` is specified, the flow detection condition is the destination IPv6 address that has been set as the IPv6 global address on the target interface.

   If `own` is specified, the flow detection conditions are the destination IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

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

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.

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 7-3: Port names that can be specified for TCP*, *Table 7-4: Port names that can be specified for UDP (IPv4)*, and *Table 7-5: Port names that can be specified for UDP (IPv6)*.

   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*>.

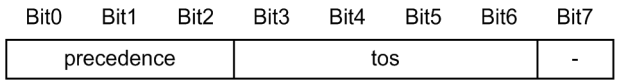
   If `range` is specified, the flow detection condition is in the range from <*destination port start*> to <*destination port end*>.

   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:

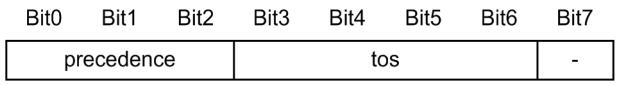
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 7-6: 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 7-7: 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:

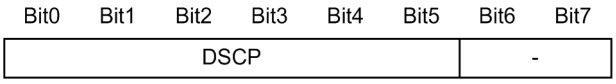
   Specify 0 to 255 in decimal.

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.

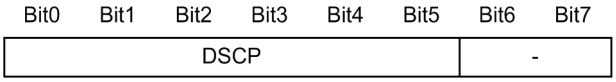
Its value is compared with the first 6 bits in the ToS field of the received packet.



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 7-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 7-11: Message names that can be specified for ICMP (IPv4)* and *Table 7-12: 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 when 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.

Fragments

Specifies the second and subsequent fragmented packets.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

■ Action parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

{user <*user id*> | llrlq1 | llrlq2} [AX6700S] [AX6600S]

Specifies a user ID set in the hierarchical shaper functionality, llrlq1, or llrlq2.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   <*user id*>: Specify 1 to 1023.

user <*user id*> [AX6300S]

Specifies a user ID set in the hierarchical shaper functionality.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   <*user id*>: Specify 1 to 511.

priority-class <*class*>

Specifies the output priority.

1. Default value when this parameter is omitted:

   The default output priority is used. For details about the default output priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

2. Range of values:

   Specify 1 to 8 (in decimal).

discard-class <*class*>

Specifies the queuing priority.

The queuing priority of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

   The default queuing priority is used. For details about the default queuing priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

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 7-8: 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 the DSCP mapping functionality, which determines the output priority and queuing priority based on the DSCP value.

For details about the output priority and queuing priority corresponding to the DSCP value, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

   None. (The DSCP mapping functionality is not used.)

2. Range of values:

   None

max-rate

Performs maximum bandwidth control.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed

the specified maximum bandwidth value are discarded.

{ <*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G }

Specifies the monitoring bandwidth value for maximum bandwidth control. Specify a value larger than `min-rate`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

max-rate-burst <*byte*>

Sets the burst size (the maximum number of bytes of the packet that exceeds the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

   3000

2. Range of values:

   <*byte*>: Specify 84 to 131072 (in decimal).

min-rate

Performs minimum bandwidth monitoring.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified monitoring bandwidth value are penalized.

Use `penalty-discard-class`, `penalty-dscp`, and `penalty-user-priority` to specify the penalty.

{<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G}

Specifies the monitoring bandwidth value for minimum bandwidth monitoring. Specify a value smaller than `max-rate`.

Note that, if the specified bandwidth exceeds the line speed, the action specified for non-compliance cannot be taken.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

min-rate-burst <*byte*>

Sets the burst size (the minimum number of bytes of the packet that falls below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

   3000

2. Range of values:

   <*byte*>: Specify 84 to 131072 (in decimal).

penalty-discard-class <*class*>

Specifies the queuing priority when non-compliance occurs in minimum bandwidth

monitoring.

The queuing priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is changed to <*class*>.

The queuing priority of compliant packets is specified with `discard-class`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify 1 to 4 (in decimal).

penalty-dscp <*dscp*>

Specifies the value for rewriting DSCP when non-compliance occurs in minimum bandwidth monitoring.

The DSCP field of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is replaced with the <*dscp*> value.

The DSCP field of compliant packets is specified with `replace-dscp`.

1. Default value when this parameter is omitted:

   None

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 7-8: DSCP names that can be specified*.

penalty-user-priority <*priority*>

Specifies the value for rewriting the user priority when non-compliance occurs in minimum bandwidth monitoring.

The user priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is replaced with the <*priority*> value.

The user priority of compliant packets is specified with `replace-user-priority`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify 0 to 7 (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. If *nnnn*`.`*nnnn*`.`*nnnn* `ffff.ffff.ffff` is entered as the source MAC address and the destination MAC address, `any` is displayed.
2. If a protocol name is set for the destination MAC address, or if the address of a protocol name

that can be set is set, the protocol name is displayed.

For details about the address of a protocol name that can be specified as the destination MAC address, see *Table 7-10: Destination MAC address names that can be specified*.

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. When `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 *nnn*.*nnn*.*nnn*.*nnn* `0.0.0.0` is entered as the source IPv4 address and the destination IPv4 address, `host` *nnn*.*nnn*.*nnn*.*nnn* is displayed.
5. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/0` is entered as the source IPv6 address and the destination IPv6 address, `any` is displayed.
6. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/128` is entered as the source address and the destination IPv6 address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn* is displayed.

Related commands

advance qos-flow-list

advance qos-flow-group

advance qos-flow-list resequence

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-list

qos (ip qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv4 QoS flow list.

Note that syntax is different if you specify fragmented packets as the detection condition. See *When "packet is fragmented" is a condition* of *Syntax*.

Note that syntax is different if you specify DSCP mapping as an action specification. See *When DSCP mapping is to be used* of *Syntax*.

Syntax

To set or change information:

[<*sequence*>] qos {flow detection condition} [action specification]

- Flow detection conditions

When "packet is not fragmented" is a condition

When the upper-layer protocol is other than TCP, UDP, ICMP, and IGMP

{ip | <*protocol*>} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*>} [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*>| <*vlan id list name*>}] [user-priority <*priority*>]

When the upper-layer protocol is TCP

tcp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | range-address <*destination ipv4 start*> <*destination ipv4 end*> } [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}][{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn|-syn}] [{urg | +urg | -urg}]}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

When the upper-layer protocol is UDP

udp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

When the upper-layer protocol is ICMP

icmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*> } [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

When the upper-layer protocol is IGMP

igmp {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*> } [<*igmp type*>] [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

When "packet is fragmented" is a condition

{ip | <*protocol*> | icmp | igmp | tcp | udp} {{<*source ipv4*> | own-address} <*source ipv4 wildcard*> | host {<*source ipv4*> | own-address} | any | own | range-address <*source ipv4 start*> <*source ipv4 end*>} {{<*destination ipv4*> | own-address} <*destination ipv4 wildcard*> | host {<*destination ipv4*> | own-address} | any | own | range-address <*destination ipv4 start*> <*destination ipv4 end*> } [{[tos <*tos*>] [precedence <*precedence*>] | dscp <*dscp*>}] [fragments] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- Action specification

For AX6700S and AX6600S series switches:

When DSCP mapping is not to be used

action

[{user <*user id*> | llrlq1 | llrlq2}]

[priority-class <*class*>] [discard-class <*class*>] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-discard-class <*class*>] [penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

When DSCP mapping is to be used

action

[{user <*user id*> | llrlq1 | llrlq2}]

[dscp-map] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

For AX6300S series switches:

When DSCP mapping is not to be used

action

[user <*user id*>]

[priority-class <*class*>] [discard-class <*class*>] [replace-dscp <*dscp*>][replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-discard-class <*class*>] [penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

When DSCP mapping is to be used

action

[user <*user id*>]

[dscp-map] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

To delete information:

no <*sequence*>

Input mode

`(config-ip-qos)`

Parameters

<*sequence*>

Sets the application sequence in the QoS flow list to be created or changed.

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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{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 7-1: Protocol names that can be specified (IPv4)*.

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

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv4*> <*source ipv4 wildcard*>, `host` <*source ipv4*>, `any`, `own-address` <*source ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*source ipv4 start*> <*source ipv4 end*>.

   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.

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

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

   `own-address` and `own` are valid only for a VLAN interface.

   If `own-address` is specified, the flow detection condition is the source IPv4 address that has been set on the target interface.

   If `own` is specified, the flow detection condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the flow detection condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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.

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 7-3: Port names that can be specified for TCP* and *Table 7-4: Port names that can be specified for UDP (IPv4)*.

   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*>.

   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 | range-address <*destination ipv4 start*> <*destination ipv4 end*>}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv4*> <*destination ipv4 wildcard*>, `host` <*destination ipv4*>, `any`, `own-address` <*destination ipv4 wildcard*>, `host own-address`, `own`, or `range-address` <*destination ipv4 start*> <*destination ipv4 end*>. 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.

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

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

   `own-address` and `own` are valid only for a VLAN interface.

   If `own-address` is specified, the flow detection condition is the destination IPv4 address that has been set on the target interface.

   If `own` is specified, the flow detection condition is the network address part of the IPv4 address that has been set on the target interface. The host address part of the IPv4 address in the flow detection condition is assumed to be arbitrary.

   If the interface with the `own-address` or `own` parameter specified is multihomed, the primary IPv4 address is assumed.

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

   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.

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 7-3: Port names that can be specified for TCP* and *Table 7-4: Port names that can be specified for UDP (IPv4)*.

   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*>.

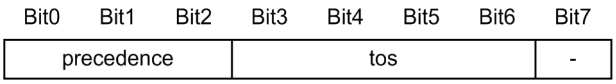
   Specify port numbers so that <*destination port end*> is larger than <*destination port start*>.

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:

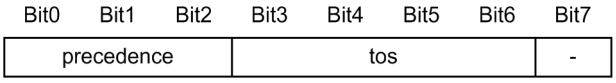
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see *Table 7-6: 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:

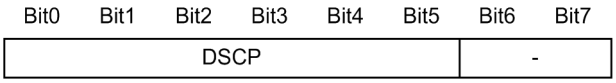
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 7-7: 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 7-8: DSCP names that can be specified*.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst` to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 7-11: 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 when 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).

Fragments

Specifies the second and subsequent fragmented packets.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

{user <*user id*> | llrlq1 | llrlq2} [AX6700S] [AX6600S]

Specifies a user ID set in the hierarchical shaper functionality, llrlq1, or llrlq2.

1. Default value when this parameter is omitted:

None

2. Range of values:

<*user id*>: Specify 1 to 1023.

user <*user id*> [AX6300S]

Specifies a user ID set in the hierarchical shaper functionality.

1. Default value when this parameter is omitted:

None

2. Range of values:

<*user id*>: Specify 1 to 511.

priority-class <*class*>

Specifies the output priority.

1. Default value when this parameter is omitted:

The default output priority is used. For details about the default output priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

2. Range of values:

Specify 1 to 8 (in decimal).

discard-class <*class*>

Specifies the queuing priority.

The queuing priority of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

The default queuing priority is used. For details about the default queuing priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

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 7-8: 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 the DSCP mapping functionality, which determines the output priority and queuing priority based on the DSCP value.

For details about the output priority and queuing priority corresponding to the DSCP value, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

None. (The DSCP mapping functionality is not used.)

2. Range of values:

None

max-rate

Performs maximum bandwidth control.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

{ <*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G }

Specifies the monitoring bandwidth value for maximum bandwidth control. Specify a value larger than `min-rate`.

1. Default value when this parameter is omitted:

None

2. Range of values:

For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

max-rate-burst <*byte*>

Sets the burst size (the maximum number of bytes of the packet that exceeds the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

3000

2. Range of values:

<*byte*>: Specify 84 to 131072 (in decimal).

min-rate

Performs minimum bandwidth monitoring.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified monitoring bandwidth value are penalized. Use `penalty-discard-class`, `penalty-dscp`, and `penalty-user-priority` to specify the penalty.

{<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G}

Specifies the monitoring bandwidth value for minimum bandwidth monitoring. Specify a value smaller than `max-rate`.

Note that, if the specified bandwidth exceeds the line speed, the action specified for

non-compliance cannot be taken.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

min-rate-burst <*byte*>

Sets the burst size (the minimum number of bytes of the packet that falls below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

   3000

2. Range of values:

   <*byte*>: Specify 84 to 131072 (in decimal).

penalty-discard-class <*class*>

Specifies the queuing priority when non-compliance occurs in minimum bandwidth monitoring.

The queuing priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is changed to <*class*>.

The queuing priority of compliant packets is specified with `discard-class`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify 1 to 4 (in decimal).

penalty-dscp <*dscp*>

Specifies the value for rewriting DSCP when non-compliance occurs in minimum bandwidth monitoring.

The DSCP field of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is replaced with the <*dscp*> value.

The DSCP field of compliant packets is specified with `replace-dscp`.

1. Default value when this parameter is omitted:

   None

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 7-8: DSCP names that can be specified*.

penalty-user-priority <*priority*>

Specifies the value for rewriting the user priority when non-compliance occurs in minimum bandwidth monitoring.

The user priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is replaced with the <*priority*> value.

The user priority of compliant packets is specified with `replace-user-priority`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify 0 to 7 (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. When `255.255.255.255` is entered for the source address wildcard mask and the destination address wildcard mask, `any` is displayed.
2. If *nnn*`.`*nnn*`.`*nnn*`.`*nnn* `0.0.0.0` is entered as the source address and the destination address, `host` *nnn*`.`*nnn*`.`*nnn*`.`*nnn* is displayed.

Related commands

ip qos-flow-list

ip qos-flow-group

ip qos-flow-list resequence

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-list

qos (ipv6 qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv6 QoS flow list.

Note that syntax is different if you specify DSCP mapping as an action specification. See *When DSCP mapping is to be used* of *Syntax*.

Syntax

To set or change information:

[<*sequence*>] qos {flow detection condition} [action specification]

- Flow detection conditions

  When the upper-layer protocol is other than TCP, UDP, and ICMP

  {ipv6 | <*protocol*>} {<*source ipv6*>/<*length*> | host <*source ipv6*> | any | own-address <*own address length*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

  When the upper-layer protocol is TCP

  tcp {<*source ipv6*>/<*length*> | host <*source ipv6*> | 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 | range-address <*destination ipv6 start*> <*destination ipv6 end*> } [{{eq | neq} <*destination port*> | range <*destination port start*> <*destination port end*>}] [{[established] | [{ack | +ack | -ack}] [{fin | +fin | -fin}] [{psh | +psh | -psh}] [{rst | +rst | -rst}] [{syn | +syn | -syn}] [{urg | +urg | -urg}]}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

  When the upper-layer protocol is UDP

  udp {<*source ipv6*>/<*length*> | host <*source ipv6*> | 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 | 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*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

  When the upper-layer protocol is ICMP

  icmp {<*source ipv6*>/<*length*> | host <*source ipv6*> | any | own-address <*own address length*>} {<*destination ipv6*>/<*length*>| host {<*destination ipv6*> | own-address} | any | own-address <*own address length*> | own | range-address <*destination ipv6 start*> <*destination ipv6 end*>} [{<*icmp type*> [<*icmp code*>] | <*icmp message*>}] [{traffic-class <*traffic class*> | dscp <*dscp*>}] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- Action specification

For AX6700S and AX6600S series switches:

When DSCP mapping is not to be used

action

[{user <*user id*> | llrlq1 | llrlq2}]

[priority-class <*class*>] [discard-class <*class*>] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-discard-class <*class*>] [penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

When DSCP mapping is to be used

action

[{user <*user id*> | llrlq1 | llrlq2}]

[dscp-map] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

For AX6300S series switches:

When DSCP mapping is not to be used

action

[user <*user id*>]

[priority-class <*class*>] [discard-class <*class*>] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-discard-class <*class*>] [penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

When DSCP mapping is to be used

action

[user <*user id*>]

[dscp-map] [replace-dscp <*dscp*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-dscp <*dscp*>] [penalty-user-priority <*priority*>]]

To delete information:

no <*sequence*>

Input mode

```
(config-ipv6-qos)
```

Parameters

<*sequence*>

Sets the application sequence in the QoS flow list to be created or changed.

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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{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 7-2: Protocol names that can be specified (IPv6)*.

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

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source ipv6*>/<*length*>, `host` <*source ipv6*>, `own-address` <*own address length*>, or `any`.

   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.

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

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

   `own-address` is valid only for a VLAN interface.

   If `own-address` is specified, the flow detection condition is the source IPv6 address that has been set as the IPv6 global address on the target interface.

   <*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.

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 7-3: Port names that can be specified for TCP* and *Table 7-5: Port names that can be specified for UDP (IPv6)*.

   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*>.

   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 | range-address <*destination ipv6 start*> <*destination ipv6 end*>}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination ipv6*>`/`<*length*>, `own-address` <*own address length*>, `host` <*destination ipv6*>, `host own-address`, `any`, `own`, or `range-address` <*destination ipv6 start*> <*destination ipv6 end*>.

   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 `own-address` that is to meet the conditions by specifying the number of bits from the start of the address.

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

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

   `own-address` and `own` are valid only for a VLAN interface.

   If `own-address` is specified, the flow detection condition is the destination IPv6 address that has been set as the IPv6 global address on the target interface.

   If `own` is specified, the flow detection conditions are the destination IPv6 address that has been set as the IPv6 global address on the target interface and the prefix length of the IPv6 global address set in <*length*>.

   If `range-address` is specified, the flow detection condition is in the range from

<*destination ipv6 start*> to <*destination ipv6 end*>.

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.

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 7-3: Port names that can be specified for TCP* and *Table 7-5: Port names that can be specified for UDP (IPv6)*.

   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*>.

   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.)

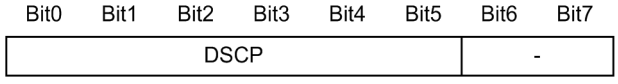
2. Range of values:

   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 7-8: DSCP names*

that can be specified.

established

Specifies 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 | -ack}

Specifies detection of packets whose ACK flag in the TCP header is 1 or 0.

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

Specify `ack` or `+ack` to detect packets whose ACK flag in the TCP header is 1. Specify `-ack` to detect packets whose ACK flag in the TCP header 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 | -fin}

Specifies detection of packets whose FIN flag in the TCP header is 1 or 0.

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

Specify `fin` or `+fin` to detect packets whose FIN flag in the TCP header is 1. Specify `-fin` to detect packets whose FIN flag in the TCP header 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 | -psh}

Specifies detection of packets whose PSH flag in the TCP header is 1 or 0.

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

Specify `psh` or `+psh` to detect packets whose PSH flag in the TCP header is 1. Specify `-psh` to detect packets whose PSH flag in the TCP header 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 | -rst}

Specifies detection of packets whose RST flag in the TCP header is 1 or 0.

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

Specify `rst` or `+rst` to detect packets whose RST flag in the TCP header is 1. Specify `-rst`

to detect packets whose RST flag in the TCP header 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 | -syn}

Specifies detection of packets whose SYN flag in the TCP header is 1 or 0.

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

Specify `syn` or `+syn` to detect packets whose SYN flag in the TCP header is 1. Specify `-syn` to detect packets whose SYN flag in the TCP header 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 | -urg}

Specifies detection of packets whose URG flag in the TCP header is 1 or 0.

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

Specify `urg` or `+urg` to detect packets whose URG flag in the TCP header is 1. Specify `-urg` to detect packets whose URG flag in the TCP header 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 7-12: 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

vlan {<*vlan id*> | <*vlan id list name*>}

Specifies the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the VLAN ID or VLAN list name.

   For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

   None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

   None

{user <*user id*> | llrlq1 | llrlq2} [AX6700S] [AX6600S]

Specifies a user ID set in the hierarchical shaper functionality, llrlq1, or llrlq2.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   <*user id*>: Specify 1 to 1023.

user <*user id*> [AX6300S]

Specifies a user ID set in the hierarchical shaper functionality.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   <*user id*>: Specify 1 to 511.

priority-class <*class*>

Specifies the output priority.

1. Default value when this parameter is omitted:

   The default output priority is used. For details about the default output priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

2. Range of values:

   Specify 1 to 8 (in decimal).

discard-class <*class*>

Specifies the queuing priority.

The queuing priority of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

   The default queuing priority is used. For details about the default queuing priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

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 7-8: 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 the DSCP mapping functionality, which determines the output priority and queuing priority based on the DSCP value.

For details about the output priority and queuing priority corresponding to the DSCP value, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

   None. (The DSCP mapping functionality is not used.)

2. Range of values:

   None

max-rate

Performs maximum bandwidth control.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

{ <*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G }

Specifies the monitoring bandwidth value for maximum bandwidth control. Specify a value larger than `min-rate`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

max-rate-burst <*byte*>

Sets the burst size (the maximum number of bytes of the packet that exceeds the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

   3000

2. Range of values:

   <*byte*>: Specify 84 to 131072 (in decimal).

min-rate

Performs minimum bandwidth monitoring.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified monitoring bandwidth value are penalized. Use `penalty-discard-class`, `penalty-dscp`, and `penalty-user-priority` to specify the penalty.

{<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G}

Specifies the monitoring bandwidth value for minimum bandwidth monitoring. Specify a value smaller than `max-rate`.

Note that, if the specified bandwidth exceeds the line speed, the action specified for non-compliance cannot be taken.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

min-rate-burst <*byte*>

Sets the burst size (the minimum number of bytes of the packet that falls below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

   3000

2. Range of values:

   <*byte*>: Specify 84 to 131072 (in decimal).

penalty-discard-class <*class*>

Specifies the queuing priority when non-compliance occurs in minimum bandwidth monitoring.

The queuing priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is changed to <*class*>.

The queuing priority of compliant packets is specified with `discard-class`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify 1 to 4 (in decimal).

penalty-dscp <*dscp*>

Specifies the value for rewriting DSCP when non-compliance occurs in minimum bandwidth monitoring.

The DSCP field of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is replaced with the <*dscp*> value.

The DSCP field of compliant packets is specified with `replace-dscp`.

1. Default value when this parameter is omitted:

   None

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 7-8: DSCP names that can be specified*.

penalty-user-priority <*priority*>

Specifies the value for rewriting the user priority when non-compliance occurs in minimum bandwidth monitoring.

The user priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is replaced with the <*priority*> value.

The user priority of compliant packets is specified with `replace-user-priority`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify 0 to 7 (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. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/0` is entered as the source address and the destination address, `any` is displayed.
2. If *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*`/128` is entered as the source address and the destination address, `host` *nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn*:*nnnn* is displayed.

Related commands

ipv6 qos-flow-list

ipv6 qos-flow-group

ipv6 qos-flow-list resequence

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-list

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 {flow detection condition} [action specification]

- Flow detection conditions

  {<*source mac*> <*source mac mask*> | host <*source mac*> | any} {<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol} [<*ethernet type*>] [vlan {<*vlan id*> | <*vlan id list name*>}] [user-priority <*priority*>]

- Action specification

For AX6700S and AX6600S series switches:

action

[{user <*user id*> | llrlq1 | llrlq2}]

[priority-class <*class*>] [discard-class <*class*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-discard-class <*class*>] [penalty-user-priority <*priority*>]]

For AX6300S series switches:

action

[user <*user id*>]

[priority-class <*class*>] [discard-class <*class*>] [replace-user-priority <*priority*>]

[max-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [max-rate-burst <*byte*>]]

[min-rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G} [min-rate-burst <*byte*>]

[penalty-discard-class <*class*>] [penalty-user-priority <*priority*>]]

To delete information:

no <*sequence*>

Input mode

```
(config-mac-qos)
```

Parameters

<*sequence*>

Specify a sequence number in the QoS flow list to be created or changed.

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 conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the source MAC address. To specify all source MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*source mac*> <*source mac mask*>, `host` <*source mac*>, or `any`. 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. If `host` <*source mac*> is specified, the flow detection condition is an exact match of <*source mac*>. If `any` is specified, the source MAC address is not used as a flow detection condition.

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

{<*destination mac*> <*destination mac mask*> | host <*destination mac*> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol}

Specifies the destination MAC address. To specify all destination MAC addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <*destination mac*> <*destination mac mask*>, `host` <*destination mac*>, `any`, `bpdu`, `cdp`, `lacp`, `lldp`, `oadp`, `pvst-plus-bpdu`, or `slow-protocol`.

   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.

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

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

   If `bpdu` is specified, BPDU control packets are used as the flow detection condition.

   If `cdp` is specified, CDP control packets are used as the flow detection condition.

   If `lacp` or `slow-protocol` is specified, slow protocol packets are used as the flow detection condition.

   This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD functionality.

   If `lldp` is specified, LLDP control packets are used as the flow detection condition.

   If `oadp` is specified, OADP control packets are used as the flow detection condition.

   If `pvst-plus-bpdu` is specified, PVST+ control packets are used as the flow detection condition.

   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 protocol names that can be specified, see *Table 7-9: Ethernet type names that can be specified*.

vlan {<*vlan id*> | <*vlan id list name*>}

Specify the VLAN ID or VLAN list name.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

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

2. Range of values:

Specify the VLAN ID or VLAN list name.

For details about the VLAN ID, see *Specifiable values for parameters*.

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 parameters

action

To set or change an action parameter, you must set the `action` parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

None. (This `action` parameter keyword cannot be omitted if an action is set.)

2. Range of values:

None

{user <*user id*> | llrlq1 | llrlq2} [AX6700S] [AX6600S]

Specifies a user ID set in the hierarchical shaper functionality, llrlq1, or llrlq2.

1. Default value when this parameter is omitted:

None

2. Range of values:

<*user id*>: Specify 1 to 1023.

user <*user id*> [AX6300S]

Specifies a user ID set in the hierarchical shaper functionality.

1. Default value when this parameter is omitted:

None

2. Range of values:

<*user id*>: Specify 1 to 511.

priority-class <*class*>

Specifies the output priority.

1. Default value when this parameter is omitted:

   The default output priority is used. For details about the default output priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

2. Range of values:

   Specify 1 to 8 (in decimal).

discard-class <*class*>

Specifies the queuing priority.

The queuing priority of the received packet is changed to the specified <*class*>.

1. Default value when this parameter is omitted:

   The default queuing priority is used. For details about the default queuing priority, see *5.10 Description of priority determination* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

2. Range of values:

   Specify 1 to 4 (in decimal).

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).

max-rate

Performs maximum bandwidth control.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

{ <*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G }

Specifies the monitoring bandwidth value for maximum bandwidth control. Specify a value larger than `min-rate`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

max-rate-burst <*byte*>

Sets the burst size (the maximum number of bytes of the packet that exceeds the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

3000

2. Range of values:

<*byte*>: Specify 84 to 131072 (in decimal).

min-rate

Performs minimum bandwidth monitoring.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified monitoring bandwidth value are penalized. Use `penalty-discard-class` and `penalty-user-priority` to specify the penalty.

{<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G}

Specifies the monitoring bandwidth value for minimum bandwidth monitoring. Specify a value smaller than `max-rate`.

Note that, if the specified bandwidth exceeds the line speed, the action specified for non-compliance cannot be taken.

1. Default value when this parameter is omitted:

None

2. Range of values:

For details about the monitoring bandwidth values that can be specified, see *Table 7-13: Message names that can be specified for ICMP (IPv6)*.

min-rate-burst <*byte*>

Sets the burst size (the minimum number of bytes of the packet that falls below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

3000

2. Range of values:

<*byte*>: Specify 84 to 131072 (in decimal).

penalty-discard-class <*class*>

Specifies the queuing priority when non-compliance occurs in minimum bandwidth monitoring.

The queuing priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is changed to <*class*>.

The queuing priority of compliant packets is specified with `discard-class`.

1. Default value when this parameter is omitted:

None

2. Range of values:

Specify 1 to 4 (in decimal).

penalty-user-priority <*priority*>

Specifies the value for rewriting the user priority when non-compliance occurs in minimum bandwidth monitoring.

The user priority of the packet that violates the minimum bandwidth monitoring conditions with `min-rate` specified is replaced with the <*priority*> value.

The user priority of compliant packets is specified with `replace-user-priority`.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Specify 0 to 7 (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. If *nnnn*.*nnnn*.*nnnn* `ffff.ffff.ffff` is entered as the source address and the destination address, `any` is displayed.
2. If a protocol name is set for the destination address or if the address of a protocol name that can be set is set, the protocol name is displayed. For details about the address of a protocol name that can be specified as the destination address, see *Table 7-10: Destination MAC address names that can be specified*. 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

mode

remark

shaper llrlq1

shaper llrlq2

shaper user

vlan-list

qos-queue-group

Sets QoS queue list information for an interface (physical port).

Syntax

To set information:

qos-queue-group <*qos queue list name*>

To delete information:

no qos-queue-group

Input mode

`(config-if)`

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 character string of no more than 31 alphanumeric characters with an alphabetic character for the first character.

Default behavior

PQ is set as the scheduling mode, and 8 is set as the number of queues.

Impact on communication

If the number of queues is changed by specifying the QoS queue list name, the corresponding line restarts, causing communication on the line stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the number of queues is changed by specifying a QoS queue list name, the new interface (a physical port) restarts. If queued packets remain in the send queue when changes are made, all packets are removed from the queue. While the packets are being removed from the queue, no new packets can be queued. You need to be careful if you logged in via a network.
2. If you did not set the scheduling mode by specifying the QoS queue list name, PQ is set as the scheduling mode.
3. If you did not set the number of queues by specifying the QoS queue list name, 8 is set as the number of queues.
4. If an invalid queue list name is specified by using the `qos-queue-group` command, PQ is used as the scheduling mode.
5. If the QoS queue list information set for the line cannot be used, an operation log message is displayed. For details about QoS queue list information that can be used, see *6.10 Correspondence between NIF models and send control functionality* in the manual *Configuration Guide Vol. 2 For Version 11.7*.
6. This command cannot be set for an interface of a NIF that does not support the legacy shaper

functionality.

7. This command cannot be set for an interface of a NIF for which the hierarchical shaper functionality has been set.

Related commands

qos-queue-list

interface gigabitethernet

interface tengigabitethernet

qos-queue-list

Sets the scheduling mode and the number of queues in QoS queue list information. You can create no more than 384 lists per device.

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 character string of no more than 31 alphanumeric characters with an alphabetic character for the first character.

{ 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 specifiable number of queues depends on the scheduling mode as follows: fixed to 8 queues, or selectable from 1, 2, 4, or 8 queues. The larger the number of a queue that runs in PQ mode is, the higher its priority is.

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. This parameter also sets the number of queues per physical port.

You can select the number of queues from 1, 2, or 4 per physical port. If you do not select the number, it is set to 8. If there are packets in multiple queues, the packets with the highest priority queue number are always sent first (for example, packets in queue 8 are sent first, followed by packets in queue 7, and so on, until queue 1 is reached).

`number_of_queue_1`: The number of queues is 1.

`number_of_queue_2`: The number of queues is 2.

`number_of_queue_4`: The number of queues is 4.

1. Default value when this parameter is omitted:

   If only `pq` is specified, the number of queues is set to 8.

rr [{ number_of_queue_1 | number_of_queue_2 | number_of_queue_4 }]

The RR scheduling mode is used. This parameter also sets the number of queues per physical port. You can select the number of queues from 1, 2, or 4 per physical port. If you do not select the number, it is set to 8. If there are packets in multiple queues, the packets in each queue are sent in turns. All queues are controlled so that they have almost the same number of packets regardless of the packet length.

`number_of_queue_1`: The number of queues is 1.

`number_of_queue_2`: The number of queues is 2.

`number_of_queue_4`: The number of queues is 4.

1. Default value when this parameter is omitted:

   If only `rr` is specified, the number of queues is set to 8.

4pq+4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>%

The 4PQ + 4WFQ scheduling mode is used. The number of queues is fixed to 8 per physical port. If 4pq (queue number 5 to 8) has packets, those packets are given the highest priority and forwarded. If 4pq has no packets, 4wfq (queue number 1 to 4) forwards packets based on the ratio of the specified weighting <*rate*>. The number that follows <*rate*> is a queue number.

1. Default value when this parameter is omitted:

   <*rate*>: This parameter cannot be omitted.

2. Range of values:

   <*rate*>: 1 to 97

   Note: These parameters must be set so that the parameters satisfy the following two formulas:

   - <*rate1*> + <*rate2*> + <*rate3*> + <*rate4*> = 100
   - <*rate1*> ≤ <*rate2*> ≤ <*rate3*> ≤ <*rate4*>

2pq+4wfq+2beq <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>%

The 2PQ + 4WFQ + 2BEQ scheduling mode is used. The number of queues is fixed to 8 per physical port. If 2pq (queue number 7 to 8) has packets, those packets are given the highest priority and forwarded. If 2pq has no packets, 4wfq (queue number 3 to 6) forwards packets based on the ratio of the specified weighting <*rate*>. If 2pq and 4wfq have no packets, 2beq (queue number 1 to 2) is operated by the PQ and forwards packets. The number that follows <*rate*> is a queue number.

1. Default value when this parameter is omitted:

   <*rate*>: This parameter cannot be omitted.

2. Range of values:

   <*rate*>: 1 to 97

   Note: These parameters must be set so that the parameters satisfy the following two formulas:

   - <*rate3*> + <*rate4*> + <*rate5*> + <*rate6*> = 100
   - <*rate3*> ≤ <*rate4*> ≤ <*rate5*> ≤ <*rate6*>

4wfq+4beq <*rate5*>% <*rate6*>% <*rate7*>% <*rate8*>%

The 4WFQ + 4BEQ scheduling mode is used. The number of queues is fixed to 8 per physical port. 4wfq (queue number 5 to 8) forwards packets based on the ratio of the specified weighting <*rate*>. If 4wfq has no packets, 4beq (queue number 1 to 4) is operated by the PQ and forwards packets. The number that follows <*rate*> is a queue number.

1. Default value when this parameter is omitted:

   <*rate*>: This parameter cannot be omitted.

2. Range of values:

   <*rate*>: 1 to 97

   Note: These parameters must be set so that the parameters satisfy the following two formulas:

   - <*rate5*> + <*rate6*> + <*rate7*> + <*rate8*> = 100
   - <*rate5*> ≤ <*rate6*> ≤ <*rate7*> ≤ <*rate8*>

Default behavior

None

Impact on communication

If the number of queues is changed by specifying the QoS queue list name for the `qos-queue-group` command, the applicable line restarts, causing communication on the line to stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the number of queues is changed by specifying the QoS queue list name for the `qos-queue-group` command, the new interface (physical port) restarts. If queued packets remain in the send queue when changes are made, all packets are removed from the queue. While the packets are being removed from the queue, no new packets can be queued. You need to be careful if you logged in via a network.
2. If the parameter for the number of queues is added, changed, or deleted from the QoS queue list information used by QoS queue interface information, the applicable interface first goes down and then comes up again.
3. If the QoS queue list information set for the line cannot be used, an operation log message is displayed. For details about QoS queue list information that can be used, see *6.10 Correspondence between NIF models and send control functionality* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

Related commands

qos-queue-group

remark

Specifies supplementary information for a QoS flow list.

There are four types of QoS flow lists: IPv4 QoS flow list, IPv6 QoS flow list, MAC QoS flow list, or Advance 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:

   The initial value is null.

2. Range of values:

   Enclose a character string of no more than 64 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

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

set-default-user-priority

Applicable shaper mode

All commands

For all the frames output from the specified NIF, the user priority is replaced with 0.

Syntax

To set information:

set-default-user-priority

To delete information:

no set-default-user-priority

Input mode

```
(config-sh-nif)
```

Parameters

None

Default behavior

The user priority is not replaced.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This functionality is applied to packets for which a value of 0x8100 or 0x9100 is set for TPID in a VLAN tag.

Related commands

shaper nif

shaper auto-configuration

Enables the shaper auto setting functionality for the device. This command cannot be set if shaper NIF information is set.

Syntax

To set or change information:

shaper auto-configuration { rgq | wgq | llpq } number-of-user <*user number*> [AX6700S] [AX6600S]

shaper auto-configuration rgq number-of-user <*user number*> [AX6300S]

To delete information:

no shaper auto-configuration

Input mode

(config)

Parameters

{ rgq | wgq | llpq } [AX6700S] [AX6600S]

Specifies the shaper mode for the shaper auto setting functionality.

rgq

Sets the bandwidth control method to RGQ. The RGQ method guarantees a minimum bandwidth for each user. Users will have the same output priority.

wgq

Sets the bandwidth control method to WGQ. WGQ method allocates bandwidth based on the ratio of the weight for each user. Users will have the same output priority.

llpq

Sets shaper mode to LLPQ1 and bandwidth control method to LLPQ. LLPQ1 method allows each user to have one queue with low delay, and guarantees a minimum bandwidth for each user. The output priority of a queue with low delay will be higher than that of a normal queue for all users. Users will have the same output priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `rgq`, `wgq`, or `llpq`.

3. Note on using this parameter:

   When the `llpq` parameter is specified, the eighth queue becomes the queue with low delay.

rgq [AX6300S]

Sets the bandwidth control method for the shaper auto setting functionality to RGQ. RGQ method guarantees a minimum bandwidth for each user. Users will have the same output priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Specify `rgq`.

number-of-user <*user number*>

Specifies the number of users per interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*user number*>: Specify from 1 to 512. [AX6700S] [AX6600S]

   <*user number*>: Specify from 1 to 256. [AX6300S]

3. Note on using this parameter [AX6700S] [AX6600S]

   If the `llpq` parameter is selected for this command, the number of users will be in the range from 1 to 256.

Default behavior

The shaper auto setting functionality is not used.

Impact on communication

When the setting is changed or deleted, the NIF is reset and communication is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This functionality is not applied to the NIF that does not support the hierarchical shaper functionality.
2. For an interface (Ethernet or VLAN), if a QoS flow list is set and a user of the hierarchical shaper functionality, llrlq1, or llrlq2 is specified in the action parameter for that QoS flow list, this functionality cannot be changed or deleted. [AX6700S] [AX6600S]
3. For an interface (Ethernet or VLAN), if a QoS flow list is specified and a user of the hierarchical shaper functionality is specified in the action parameter for that QoS flow list, this functionality cannot be changed or deleted. [AX6300S]

Related commands

shaper nif

shaper vlan-user-map

shaper default-user

Applicable shaper modes

All shaper modes

Applies a user list and enables the default user for an Ethernet interface.

This command cannot be set if shaper mode is not set for the NIF for the interface. Also, this command cannot be set if the shaper auto setting functionality is used, or if the number of ports exceeds the allowed number of ports for the shaper functionality.

Syntax

To set or change information:

shaper default-user list <*user list name*>

To delete information:

no shaper default-user

Input mode

`(config-if)`

Parameters

list <*user list name*>

Specifies a user list name to be used for the default user.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*user list name*>: Specify a name that has no more than 31 characters, and without a numeric character used for the first character.

   - Specify the user list name that has been created by the `shaper user-list` command.

3. Note on using this parameter:

   - This parameter cannot be set if the total of the minimum bandwidth values for all users and the default user that have been set for the target interface exceeds the port bandwidth control value (applicable shaper modes: [rgq], [llpq1], [llpq2], and [llpq4]).

   - This parameter cannot be set if the total of the minimum bandwidth values for all users and the default user that have been set for the target interface and the maximum bandwidth values for llrlq1 and llrlq2 exceeds the port bandwidth control value (applicable shaper modes: [rgq llrlq], [llpq1 llrlq], [llpq2 llrlq], and [llpq4 llrlq]). [AX6700S] [AX6600S]

   - This parameter cannot be set if the setting contents of the specified user list are not suitable for the shaper mode set for the NIF for the target interface. For details about the restriction of the setting contents, see the command relating to user list.

Default behavior

The default user is not set for the target interface.

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 interface of a NIF that does not support the hierarchical shaper functionality.

Related commands

shaper nif

shaper user-list

shaper llrlq1 [AX6700S] [AX6600S]

Applicable shaper modes

[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

Applies a user list and enables llrlq1 for an Ethernet interface. This command cannot be set if the target shaper mode is not set for the NIF for the interface. Also, this command cannot be set if the shaper auto setting functionality is used, or if the number of ports exceeds the allowed number of ports for the shaper functionality.

Syntax

To set or change information:

shaper llrlq1 list <*user list name*>

To delete information:

no shaper llrlq1

Input mode

`(config-if)`

Parameters

list <*user list name*>

Specifies a user list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*user list name*>: Specify a name that has no more than 31 characters, and without a numeric character used for the first character.

   - Specify the user list name that has been created by the `shaper user-list` command.

3. Note on using this parameter:

   This parameter cannot be specified if the total of the maximum bandwidth values for the specified user list, the maximum bandwidth values for llrlq2 set for the target interface, and the minimum bandwidth values for all users and the default user exceeds the port bandwidth control value (applicable shaper modes: [rgq llrlq], [llpq1 llrlq], [llpq2 llrlq], and [llpq4 llrlq]).

   This parameter cannot be specified if the total of the maximum bandwidth value for the specified user list and the maximum bandwidth value for llrlq2 set for the target interface exceeds the port bandwidth control value (applicable shaper mode: [wgq llrlq]).

   - This parameter cannot be set if the setting contents of the specified user list are not suitable for the shaper mode set for the NIF for the target interface. For details about the restriction of the setting contents, see the command relating to user list.

Default behavior

llrlq1 is not set for the target interface.

Impact on communication

When the setting is changed or deleted, communication for llrlq1 is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an interface of a NIF that does not support the hierarchical shaper functionality.

Related commands

shaper nif

shaper user-list

shaper llrlq2 [AX6700S] [AX6600S]

Applicable shaper modes

[rgq llrlq] [wgq llrlq] [llpq1 llrlq] [llpq2 llrlq] [llpq4 llrlq]

Applies a user list and enables llrlq2 for an Ethernet interface. This command cannot be set if the target shaper mode is not set for the NIF for the interface. Also, this command cannot be set if the shaper auto setting functionality is used, or if the number of ports exceeds the allowed number of ports for the shaper functionality.

Syntax

To set or change information:

shaper llrlq2 list <*user list name*>

To delete information:

no shaper llrlq2

Input mode

`(config-if)`

Parameters

list <*user list name*>

Specifies a user list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*user list name*>: Specify a name that has no more than 31 characters, and without a numeric character used for the first character.

   - Specify the user list name that has been created by the `shaper user-list` command.

3. Note on using this parameter:

   This parameter cannot be specified if the total of the maximum bandwidth values for the specified user list, the maximum bandwidth values for llrlq1 set for the target interface, and the minimum bandwidth values for all users and the default user exceeds the port bandwidth control value (applicable shaper modes: [rgq llrlq], [llpq1 llrlq], [llpq2 llrlq], and [llpq4 llrlq]).

   This parameter cannot be specified if the total of the maximum bandwidth value for the specified user list and the maximum bandwidth value for llrlq2 set for the target interface exceeds the port bandwidth control value (applicable shaper mode: [wgq llrlq]).

   - This parameter cannot be set if the setting contents of the specified user list are not suitable for the shaper mode set for the NIF for the target interface. For details about the restriction of the setting contents, see the command relating to user list.

Default behavior

llrlq2 is not set for the target interface.

Impact on communication

When the setting is changed or deleted, communication for llrlq2 is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an interface of a NIF that does not support the hierarchical shaper functionality.

Related commands

shaper nif

shaper user-list

shaper nif

Sets shaper NIF information. This command cannot be set if the shaper auto setting functionality is used. Entering this command switches to `config-sh-nif` mode in which information about the relevant shaper NIF can be set.

Syntax

To set or change information:

shaper nif <*nif list*>

To delete information:

no shaper nif <*nif list*>

Input mode

`(config)`

Parameters

<*nif list*>

Specifies a NIF number. Multiple NIF numbers can be specified by using a hyphen (-) or a comma (,). You can also specify one NIF number, as when <*nif no.*> is written.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See the range of <*nif no.*> in *Specifiable values for parameters*.

Default behavior

Shaper NIF information is not set.

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 a NIF that does not support the hierarchical shaper functionality. Also, this command cannot be set for a NIF for which legacy shaper functionality has been set.

Related commands

None

shaper port buffer

Applicable shaper modes

All shaper modes

Sets the buffer capacity for each queue used for port bandwidth control for an Ethernet interface.

This command cannot be set if shaper mode is not set for the NIF for the interface. Also, this command cannot be set if the shaper auto setting functionality is used, or if the number of ports exceeds the allowed number of ports for the shaper functionality.

Syntax

To set or change information:

shaper port buffer <*qos1*> <*qos2*> <*qos3*> <*qos4*> [<*qos5*> <*qos6*> <*qos7*> <*qos8*>]

To delete information:

no shaper port buffer

Input mode

```
(config-if)
```

Parameters

<*qos1*> <*qos2*> <*qos3*> <*qos4*> [<*qos5*> <*qos6*> <*qos7*> <*qos8*>]

Specifies the buffer capacity.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*qos*>: Specify 0 to 96000. [AX6700S] [AX6600S]

   - <*qos*>: Specify 0 to 48000. [AX6300S]

   - <*qos1*> to <*qos4*> can be set for 4-queue mode.

   - <*qos1*> to <*qos8*> can be set for 8-queue mode.

Default behavior

The buffer value for each queue used for port bandwidth control is set based on the default value. For details about the default value, see *6.7.2 Buffer management* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

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 interface of a NIF that does not support the hierarchical shaper functionality.
2. If the set <*qos*> value exceeds the upper limit of the buffer capacity per NIF, the upper limit value is applied to the device. [AX6300S]
3. During 4-queue mode operation, if values are set for <*qos1*> to <*qos8*>, the values set for

<*qos1*> to <*qos4*> are applied, and the values set for <*qos5*> to <*qos8*> are ignored.

4. During 8-queue mode operation, if values are not set for <*qos5*> to <*qos8*>, the values set for <*qos1*> to <*qos4*> are ignored, and the initial values are set for <*qos1*> to <*qos8*>.

Related commands

shaper nif

shaper port rate-limit

Applicable shaper modes

All shaper modes

Sets port bandwidth control for an Ethernet interface.

This command cannot be set if shaper mode is not set for the NIF for the interface. Also, this command cannot be set for the target interface if the shaper auto setting functionality is used, or if the number of ports exceeds the allowed number of ports for the shaper functionality.

Syntax

To set or change information:

shaper port rate-limit { <*kbit/s*> | <*Mbit/s*>M }

To delete information:

no shaper port rate-limit

Input mode

```
(config-if)
```

Parameters

{ <*kbit/s*> | <*Mbit/s*>M }

Specifies a port bandwidth control value. Using this functionality enables you to limit the line send bandwidth to the specified bandwidth.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See the table below.

   M can be specified as the unit of values.

   Set the bandwidth so that it is equal to or smaller than the line speed.

Table 7-21: Setting range for a port bandwidth control value

Line speed (including auto-negotiation results)	Setting range		Increment
1000 Mbit/s	In Mbit/s	1 M to 1000 M	1 Mbit/s
	In kbit/s	64 to 1000000	1 kbit/s
100 Mbit/s	In Mbit/s	1 M to 100 M	1 Mbit/s
	In kbit/s	64 to 100000	1 kbit/s
10 Mbit/s	In Mbit/s	1 M to 10 M	1 Mbit/s
	In kbit/s	64 to 10000	1 kbit/s

3. Note on using this parameter:

   - No values smaller than the total of the minimum bandwidth values for all users and the default user that have been set for the target interface can be set (applicable shaper modes: [rgq], [llpq1], [llpq2], and [llpq4]).

   - If llrlq1 or llrlq2 is set for an interface, no values smaller than the total of the maximum

bandwidth values for llrlq1 and llrlq2 that are set for the interface and the minimum bandwidth values for all users and the default user can be set (applicable shaper modes: [rgq llrlq], [llpq1 llrlq], [llpq2 llrlq], and [llpq4 llrlq]). [AX6700S] [AX6600S]

- If llrlq1 or llrlq2 is set for an interface, no values smaller than the total of the maximum bandwidth values for llrlq1 and llrlq2 that are set for the interface can be set (applicable shaper mode: [wgq llrlq]). [AX6700S] [AX6600S]

If the `shaper wgq-group rate-limit` command is set for an interface, no values smaller than the value set by the `shaper wgq-group rate-limit` command can be set. [AX6700S] [AX6600S]

Default behavior

The port bandwidth control value is set to 1000 M.

Impact on communication

When the setting is changed or deleted, ports are deactivated and communication is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an interface of a NIF that does not support the hierarchical shaper functionality.

Related commands

shaper nif

shaper user

Applicable shaper modes

All shaper modes

Applies a user list and enables users for an Ethernet interface.

This command cannot be set if shaper mode is not set for the NIF for the interface. Also, this command cannot be set if the shaper auto setting functionality is used, or if the number of ports exceeds the allowed number of ports for the shaper functionality.

Syntax

To set information:

shaper user <*user id list*> list <*user list name*>

To change information:

shaper user { <*user id list*> | add <*user id list*> } list <*user list name*>

shaper user remove <*user id list*>

To delete information:

no shaper user

Input mode

`(config-if)`

Parameters

<*user id list*>

Specifies user IDs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - Specify 1 to 1023. The range of the specifiable user IDs depends on the shaper mode and the number of queues. If the specified user ID is outside the valid setting range, the user ID is not applied to the device. [AX6700S] [AX6600S]

   - Specify 1 to 511. The range of the specifiable user IDs depends on the number of queues. If the specified user ID is outside the valid setting range, the user ID is not applied to the device. [AX6300S]

   - The same IDs cannot be set for an interface.

list <*user list name*>

Specifies a user list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*user list name*>: Specify a name that has no more than 31 characters, and without a numeric character used for the first character.

   - Specify the user list name that has been created by the `shaper user-list` command.

3. Note on using this parameter:

- This parameter cannot be set if the total of the minimum bandwidth values for all users and the default user that have been set for the target interface exceeds the port bandwidth control value (applicable shaper modes: [rgq], [llpq1], [llpq2], and [llpq4]).

- This parameter cannot be set if the total of the minimum bandwidth values for all users and the default user that have been set for the target interface and the maximum bandwidth values for llrlq1 and llrlq2 exceeds the port bandwidth control value (applicable shaper modes: [rgq llrlq], [llpq1 llrlq], [llpq2 llrlq], and [llpq4 llrlq]). [AX6700S] [AX6600S]

- This parameter cannot be set if the setting contents of the specified user list are not suitable for the shaper mode set for the NIF for the target interface. For details about the restriction of the setting contents, see the command relating to user list.

add <*user id list*>

Add user IDs to the user list that has been specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - Specify 1 to 1023. The range of the specifiable user IDs depends on the shaper mode and the number of queues. If the specified user ID is outside the valid setting range, the user ID is not applied to the device. [AX6700S] [AX6600S]

   - Specify 1 to 511. The range of the specifiable user IDs depends on the number of queues. If the specified user ID is outside the valid setting range, the user ID is not applied to the device. [AX6300S]

   - The same IDs cannot be set for an interface.

3. Handling of <*user id list*> after a change:

   If adding user IDs makes the user list long, the user list might be split and the configuration might be displayed as `shaper user` commands on multiple lines. Conversely, if the user list is short after user IDs are added, the configuration might be displayed with the user list consolidated with several `shaper user` commands on multiple lines.

remove <*user id list*>

Removes user IDs from the user list that has been specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - Specify 1 to 1023. Only the user IDs that have been specified in the user list can be removed. You can remove multiple user lists. [AX6700S] [AX6600S]

   - Specify 1 to 511. Only the user IDs that have been specified in the user list can be removed. You can remove multiple user lists. [AX6300S]

3. Handling of <*user id list*> after a change:

   If deleting user IDs makes the user list long, the user list might be split and the configuration might be displayed as `shaper user` commands on multiple lines. Conversely, if the user list is short after user IDs are deleted, the configuration might be displayed with the user list consolidated with several `shaper user` commands on multiple lines.

Default behavior

Users are not set for the target interface.

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 interface of a NIF that does not support the hierarchical shaper functionality.

Related commands

shaper nif

shaper user-list

shaper user-list

Applicable shaper mode

All commands

Creates a user list. You can create no more than 8192 lists per device.

Syntax

To set or change information:

shaper user-list <*user list name*> [peak-rate {<*kbit/s*> | <*Mbit/s*>M} [min-rate {<*kbit/s*> | <*Mbit/s*>M} [llpq-peak-rate {<*kbit/s*> | <*Mbit/s*>M}]]] [weight <*weight*>] [{

pq |

llq+3wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

pq+llq+2wfq <*rate1*>% <*rate2*>% <*rate3*>% |

2pq+llq+4wfq+beq <*rate2*>% <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>% |

4pq+4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

2pq+4wfq+2beq <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>% }]

[queue-length <*length1*> <*length2*> <*length3*> <*length4*> [<*length5*> <*length6*> <*length7*> <*length8*>]] [discard <*queue1*> <*queue2*> <*queue3*> <*queue4*> [<*queue5*> <*queue6*> <*queue7*> <*queue8*>]] [AX6700S] [AX6600S]

shaper user-list <*user list name*> [peak-rate {<*kbit/s*> | <*Mbit/s*>M} [min-rate {<*kbit/s*> | <*Mbit/s*>M}]] [weight <*weight*>] [{

pq |

llq+3wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

pq+llq+2wfq <*rate1*>% <*rate2*>% <*rate3*>% |

2pq+llq+4wfq+beq <*rate2*>% <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>% |

4pq+4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

2pq+4wfq+2beq <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>% }]

[queue-length <*length1*> <*length2*> <*length3*> <*length4*> [<*length5*> <*length6*> <*length7*> <*length8*>]] [discard <*queue1*> <*queue2*> <*queue3*> <*queue4*> [<*queue5*> <*queue6*> <*queue7*> <*queue8*>]] [AX6300S]

To delete information:

no shaper user-list <*user list name*>

Input mode

```
(config)
```

Parameters

<*user list name*>

Specifies a user list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*user list name*>: Specify a name that has no more than 31 characters, and without a numeric character used for the first character.

3. Note on using this parameter:

   None

peak-rate {<*kbit/s*> | <*Mbit/s*>M}

Specifies the maximum bandwidth.

1. Default value when this parameter is omitted:

   The maximum bandwidth is not set.

2. Range of values:

   - <*kbit/s*>: Specify 64 to 1000000.

   - <*Mbit/s*>: Specify 1 M to 1000 M.

3. Note on using this parameter:

   - For a user or for the default user on an interface for which the applicable shaper mode is set, specify the maximum bandwidth. If the maximum bandwidth is not specified, the user list will not be applied to the device (applicable shaper mode: [rgq], [rgq llrlq], [llpq1], [llpq1 llrlq], [llpq2], [llpq2 llrlq], [llpq4], or [llpq4 llrlq]).

   - If the maximum bandwidth is not specified for the user list that is to be set for llrlq1 or llrlq2, the user list will not be applied to the device. [AX6700S] [AX6600S]

   - You cannot set a value smaller than the minimum bandwidth value set for the user list.

   - You cannot set a value smaller than the LLPQ bandwidth control value set for the user list.

   - For the maximum bandwidth of the user list that is to be set for a user or for the default user on an interface, set a value no more than the port bandwidth control value set for the interface.

   - If the maximum bandwidth is set for the user list that is to be set for a user or for the default user on an interface for which the applicable shaper mode is set, the maximum bandwidth will not be applied to the device (applicable shaper mode: [wgq] or [wgq llrlq]). [AX6700S] [AX6600S]

   - If the total of the maximum bandwidth values for llrlq1 and llrlq2 on an interface for which the applicable shaper mode is set exceeds the port bandwidth control value set for the interface, you cannot set such values for the maximum bandwidth (applicable shaper mode: [wgq llrlq]). [AX6700S] [AX6600S]

   - If the total of the maximum bandwidth values for llrlq1 and llrlq2 on an interface for which the applicable shaper mode is set and the minimum bandwidth values for all users and the default user exceeds the port bandwidth control value set for the interface, you cannot set such values for the maximum bandwidth value (applicable shaper mode: [rgq llrlq], [llpq1 llrlq], [llpq2 llrlq], or [llpq4 llrlq]). [AX6700S] [AX6600S]

min-rate {<*kbit/s*> | <*Mbit/s*>M}

Specifies the minimum bandwidth.

1. Default value when this parameter is omitted:

   The minimum bandwidth is not set.

2. Range of values:

   - <*kbit/s*>: Specify 64 to 1000000.

   - <*Mbit/s*>: Specify 1 M to 1000 M.

3. Note on using this parameter:

   - For a user or for the default user on an interface for which the applicable shaper mode is set, specify the minimum bandwidth. If the minimum bandwidth is not specified, the user list will not be applied to the device (applicable shaper mode: [rgq], [rgq llrlq], [llpq1], [llpq1 llrlq], [llpq2], [llpq2 llrlq], [llpq4], or [llpq4 llrlq]).

   - You cannot set a value larger than the maximum bandwidth value set for the user list.

   - If the minimum bandwidth is set for the user list that is to be set for a user or for the default user on an interface for which the applicable shaper mode is set, the minimum bandwidth will not be applied to the device (applicable shaper mode: [wgq] or [wgq llrlq]). [AX6700S] [AX6600S]

   - If the minimum bandwidth is set for the user list that is to be set for llrlq1 or llrlq2, the minimum bandwidth will not be applied to the device. [AX6700S] [AX6600S]

   - If the user list is set for an interface, and if the total of the minimum bandwidth values for users and for the default user that are set on the interface exceeds the port bandwidth control value, you cannot set such values for the minimum bandwidth (applicable shaper mode: [rgq], [llpq1], [llpq2], or [llpq4]).

   - If the user list is set for an interface, and if the total of the minimum bandwidth values for users and for the default user that are set on the interface and the maximum bandwidth values for llrlq1 and llrlq2 exceeds the port bandwidth control value, you cannot set such values for the minimum bandwidth (applicable shaper mode: [rgq llrlq], [llpq1 llrlq], [llpq2 llrlq], or [llpq4 llrlq]). [AX6700S] [AX6600S]

llpq-peak-rate {<*kbit/s*> | <*Mbit/s*>M} [AX6700S] [AX6600S]

Specifies LLPQ bandwidth control.

1. Default value when this parameter is omitted:

   The maximum bandwidth value for the queues with low delay will be the same as the minimum bandwidth value set in the user list.

2. Range of values:

   - <*kbit/s*>: Specify 64 to 1000000.

   - <*Mbit/s*>: Specify 1 M to 1000 M.

3. Note on using this parameter:

   - This parameter cannot be set if the user list has no setting for the minimum bandwidth.

   - You cannot set a value larger than the maximum bandwidth value set for the user list.

   - If LLPQ bandwidth control is set for the user list that is to be set for llrlq1 or llrlq2, LLPQ bandwidth control will not be applied to the device.

   - If LLPQ bandwidth control is set for the user list that is to be set for a user or for the default user on an interface for which the applicable shaper mode is set, LLPQ bandwidth control will not be applied to the device (applicable shaper mode: [rgq], [rgq llrlq], [wgq], or [wgq llrlq]).

weight <*weight*>

Specifies the weight for distributing bandwidth.

1. Default value when this parameter is omitted:

The weight for distributing bandwidth is set to 1.

2. Range of values:

   Specify 1 to 50.

3. Note on using this parameter:

   - If the weight value is specified for a user list set for llrlq1 or llrlq2 on an interface for which the applicable shaper mode is set, the weight value will not be applied to the device. [AX6700S] [AX6600S]

   - If 11 or more is specified for the weight value of a user list set for a user or for the default user on an interface for which the applicable shaper mode is set, 10 will be applied as the weight value to the device (applicable shaper mode: [wgq] or [wgq llrlq]). [AX6700S] [AX6600S]

   - If the same value is set for `peak-rate` and `min-rate` of a user list for a user or for the default user on an interface for which the applicable shaper mode is set, the weight value will not be applied to the device (applicable shaper mode: [rgq], [rgq llrlq], [llpq1], [llpq1 llrlq], [llpq2], [llpq2 llrlq], [llpq4], or [llpq4 llrlq]).

{ pq |

llq+3wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

pq+llq+2wfq <*rate1*>% <*rate2*>% <*rate3*>% |

2pq+llq+4wfq+beq <*rate2*>% <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>% |

4pq+4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>% |

2pq+4wfq+2beq <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>% }

Specifies the scheduling mode. The scheduling modes that can be set depend on the number of queues for a user set for the NIF.

4-queue mode: pq, llq+3wfq, 4wfq, or pq+llq+2wfq

8-queue mode: pq, 2pq+llq+4wfq+beq, 4pq+4wfq, or 2pq+4wfq+2beq

pq

Sends packets by using complete priority queuing.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

3. Note on using this parameter [AX6700S] [AX6600S]

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queue with the highest priority will be the low-delay queue, which has LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq1] or [llpq1 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, there will be two high-priority low-delay queues, which have LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq2] or [llpq2 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, there will be four high-priority low-delay

queues, which have LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq4] or [llpq4 llrlq]).

llq+3wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>%

In the fourth queue (llq), the specified rate of the packets is given the highest priority for output. For the first to third queues (3wfq), weighted fair queuing is used, where the remaining bandwidth after the bandwidth used by the fourth queue (not the set bandwidth) is subtracted from users' send bandwidth, is shared among the queues based on their weights.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*rate1*> to <*rate3*>: Specify 1 to 100. When you specify the values, make sure that the following condition is satisfied and the total value of <*rate*> is no more than 100: <*rate1*> = <*rate2*> = <*rate3*>.

   - <*rate4*>: Specify 5 to 100. Note that you can specify the value in increments of 5. If 100 is specified, the fourth queue operates as priority queueing.

3. Note on using this parameter [AX6700S] [AX6600S]

   - When this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queue with the highest priority will be the low-delay queue, which has LLPQ bandwidth control set for the maximum bandwidth, only if 100 is set for <*rate4*>. If a value other than 100 is set for <*rate4*>, the queues operate as pq (applicable shaper mode: [llpq1] or [llpq1 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queues operate as pq (applicable shaper mode: [llpq2], [llpq2 llrlq], [llpq4], or [llpq4 llrlq]).

4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>%

Weighted fair queuing is used for the queues, where the bandwidth is shared among the queues based on their weights.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*rate1*> to <*rate4*>: Specify 1 to 100. When you specify the values, make sure that the following condition is satisfied and the total value of <*rate*> is no more than 100: <*rate1*> = <*rate2*> = <*rate3*> = <*rate4*>.

3. Note on using this parameter [AX6700S] [AX6600S]

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queues operate as pq (applicable shaper mode: [llpq1], [llpq1 llrlq], [llpq2], [llpq2 llrlq], [llpq4], or [llpq4 llrlq]).

pq+llq+2wfq <*rate1*>% <*rate2*>% <*rate3*>%

The fourth queue (pq) operates with priority queueing, which outputs packets with highest priority. The remaining bandwidth, after the bandwidth used by the fourth queue is subtracted from users' send bandwidth, is allocated as follows: The specified proportion of the remaining bandwidth is used for the third queue (llq) priority traffic. Queues 1 and 2 share the rest according to their weighting (2wfq).

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   - <*rate1*> to <*rate2*>: Specify 1 to 100. When you specify the values, make sure that the following condition is satisfied and the total value of <*rate*> is no more than 100: <*rate1*> = <*rate2*>.

   - <*rate3*>: Specify 5 to 100. Note that you can specify the value in increments of 5. If 100 is specified, the third queue operates as priority queueing.

3. Note on using this parameter [AX6700S] [AX6600S]

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queue with the highest priority will be the low-delay queue, which has LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq1] or [llpq1 llrlq]).

   - When this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, two queues with high priority will be the low-delay queues, which have LLPQ bandwidth control set for the maximum bandwidth, only if 100 is set for <*rate3*>. If a value other than 100 is set for <*rate3*>, the queues operate as pq (applicable shaper mode: [llpq2] or [llpq2 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queues operate as pq (applicable shaper mode: [llpq4] or [llpq4 llrlq]).

2pq+llq+4wfq+beq <*rate2*>% <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>%

The seventh and eighth queues (2pq) operate with priority queuing, which outputs packets with highest priority. The remaining bandwidth, after the bandwidth used by the seventh and eighth queues is subtracted from users' send bandwidth, is allocated as follows: The specified proportion of the remaining bandwidth is used for sixth queue (llq) priority traffic. Queues 2 to 5 share the rest according to their weighting (4wfq). The remaining bandwidth is used by the first queue (beq).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*rate2*> to <*rate5*>: Specify 1 to 100. When you specify the values, make sure that the following condition is satisfied and the total value of <*rate*> is no more than 100: <*rate2*> = <*rate3*> = <*rate4*> = <*rate5*>.

   - <*rate6*>: Specify 5 to 100. Note that you can specify the value in increments of 5. If 100 is specified, the sixth queue operates as priority queueing.

3. Note on using this parameter [AX6700S] [AX6600S]

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queue with the highest priority will be the low-delay queue, which has LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq1], [llpq1 llrlq], [llpq2], or [llpq2 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, there will be two high-priority low-delay queues, which have LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq2] or [llpq2 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queues operate as pq (applicable shaper mode: [llpq4] or [llpq4 llrlq]).

4pq+4wfq <*rate1*>% <*rate2*>% <*rate3*>% <*rate4*>%

The fifth to eighth queues (4pq) operate with priority queuing, which outputs packets with highest priority. For the remaining bandwidth, after the bandwidth used by the fifth to eighth queues (not the set bandwidth) is subtracted from users' send bandwidth, weighted fair queuing is used. Therefore, queues 1 to 4 are guaranteed to share the remaining bandwidth according to their weighting (4wfq).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*rate1*> to <*rate4*>: Specify 1 to 100. When you specify the values, make sure that the following condition is satisfied and the total value of <*rate*> is no more than 100: <*rate1*> = <*rate2*> = <*rate3*> = <*rate4*>.

3. Note on using this parameter [AX6700S] [AX6600S]

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queue with the highest priority will be the low-delay queue, which has LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq1] or [llpq1 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, there will be two high-priority low-delay queues, which have LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq2] or [llpq2 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, there will be four high-priority low-delay queues, which have LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq4] or [llpq4 llrlq]).

2pq+4wfq+2beq <*rate3*>% <*rate4*>% <*rate5*>% <*rate6*>%

The seventh and eighth queues (2pq) operate with priority queuing, which outputs packets with highest priority. The remaining bandwidth, after the bandwidth used by the seventh and eighth queues (not the set bandwidth) is subtracted from users' send bandwidth, is allocated as follows: For queues 3 to 6, weighted fair queuing is used, where queues are guaranteed to share the remaining bandwidth according to their weighting (4wfq). The remaining bandwidth is used by the first and second queues (2beq).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*rate3*> to <*rate6*>: Specify 1 to 100. When you specify the values, make sure that the following condition is satisfied and the total value of <*rate*> is no more than 100: <*rate3*> = <*rate4*> = <*rate5*> = <*rate6*>. Specify the maximum bandwidth for the user list.

3. Note on using this parameter [AX6700S] [AX6600S]

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queue with the highest priority will be the low-delay queue, which has LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq1] or [llpq1 llrlq]).

   - If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, there will be two high-priority low-delay

queues, which have LLPQ bandwidth control set for the maximum bandwidth (applicable shaper mode: [llpq2] or [llpq2 llrlq]).

- If this parameter is specified for a user or for the default user on an interface for which the applicable shaper mode is set, the queues operate as pq (applicable shaper mode: [llpq4] or [llpq4 llrlq]).

1. Default value when this parameter is omitted:

   The scheduling mode will be pq.

2. Range of values:

   pq, llq+3wfq, 4wfq, pq+llq+2wfq, 2pq+llq+4wfq+beq, 4pq+4wfq, or 2pq+4wfq+2beq

3. Note on using this parameter:

   If the specified scheduling mode does not match the queue mode, the scheduling mode will be pq.

queue-length <*length1*> <*length2*> <*length3*> <*length4*> [<*length5*> <*length6*> <*length7*> <*length8*>]

Specifies the queue length for each queue.

1. Default value when this parameter is omitted:

   The queue length of each queue is set according to the default value. For details about the default value, see *6.7.2 Buffer management* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

2. Range of values:

   - <*length*>: Specify 0 to 4000.

   - <*length1*> to <*length4*> can be set for 4-queue mode.

   - <*length1*> to <*length8*> can be set for 8-queue mode.

3. Note on using this parameter:

   - During 4-queue mode operation, if values are set for <*length1*> to <*length8*>, the values set for <*length1*> to <*length4*> are applied, and the values set for <*length5*> to <*length8*> are ignored.

   - During 8-queue mode operation, if values are not set for <*length5*> to <*length8*>, the values set for <*length1*> to <*length4*> are ignored, and the initial values are set for <*length1*> to <*length4*>.

discard <*queue1*> <*queue2*> <*queue3*> <*queue4*> [<*queue5*> <*queue6*> <*queue7*> <*queue8*>]

Specifies the drop control mode for each queue.

1. Default value when this parameter is omitted:

   Each queue operates in tail-drop2 mode.

2. Range of values:

   - <*queue*>: Specify tail-drop1, tail-drop2, or tail-drop3.

   - <*queue1*> to <*queue4*> can be set for 4-queue mode.

   - <*queue1*> to <*queue8*> can be set for 8-queue mode.

   The following table lists the discard threshold value corresponding to each discard mode.

Table 7-22: Drop threshold values corresponding to the discard modes

Discard mode	Queuing priority	
	1 to 2	3 to 4
tail-drop1	1/4	4/4
tail-drop2	2/4	4/4
tail-drop3	3/4	4/4

3. Note on using this parameter:

   - During 4-queue mode operation, if values are set for <*queue1*> to <*queue8*>, the values set for <*queue1*> to <*queue4*> are applied, and the values set for <*queue5*> to <*queue8*> are ignored.

   - During 8-queue mode operation, if values are not set for <*queue5*> to <*queue8*>, the values set for <*queue1*> to <*queue4*> are ignored, and the initial values are set for <*queue1*> to <*queue4*>.

Default behavior

No user list is created.

Impact on communication

When the setting for a user list that has been set for an interface is changed, communication for the target user is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

shaper nif

shaper vlan-user-map

Sets VLAN user mapping on the device. If this command is set, queuing is performed based on the header information in the VLAN tag. Queuing is not performed based on priority determination for the QoS flow list.

Syntax

To set or change information:

shaper vlan-user-map [user-priority-queue-map <*priority0*> <*priority1*> <*priority2*> <*priority3*> <*priority4*> <*priority5*> <*priority6*> <*priority7*>]

To delete information:

no shaper vlan-user-map

Input mode

(config)

Parameters

user-priority-queue-map <*priority0*> <*priority1*> <*priority2*> <*priority3*> <*priority4*> <*priority5*> <*priority6*> <*priority7*>

Configures user priority queue mapping. Specify the queue numbers for <*priority0*> to <*priority7*> that correspond to the user priority 0 to 7.

1. Default value when this parameter is omitted:

   <*priority0*>: 3

   <*priority1*>: 1

   <*priority2*>: 2

   <*priority3*>: 4

   <*priority4*>: 5

   <*priority5*>: 6

   <*priority6*>: 7

   <*priority7*>: 8

2. Range of values:

   <*priority0*> to <*priority7*>: Specify 1 to 8.

3. Note on using this parameter:

   The number of the queue that is queued depends on the number of queues operating on a shaper NIF. The following table lists the number of the queue that is queued.

Table 7-23: Number of the queue that is queued

Queue number specified in this parameter	Number of the queue that is queued during 8-queue operation (default)	Number of the queue that is queued during 4-queue operation
1	1	1
2	2	
3	3	2
4	4	

Queue number specified in this parameter	Number of the queue that is queued during 8-queue operation (default)	Number of the queue that is queued during 4-queue operation
5	5	3
6	6	
7	7	4
8	8	

Default behavior

VLAN user mapping is not used.

Impact on communication

When the setting is changed or deleted, the NIF is reset and communication is disconnected temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This functionality is not applied to the NIF that does not support the hierarchical shaper functionality.
2. This functionality is applied to packets for which a value of 0x8100 or 0x9100 is set for TPID in a VLAN tag.
3. This functionality is not applied to a NIF to which the shaper auto setting functionality or shaper mode has not been applied.

Related commands

shaper nif

shaper auto-configuration

shaper wgq-group rate-limit [AX6700S] [AX6600S]

Applicable shaper mode

[wgq llrlq]

Specifies WGQ bandwidth control for the total bandwidth used by all users for the target interface of the Ethernet interface. This command cannot be set if shaper mode is not set for the NIF for the interface.

Syntax

To set or change information:

shaper wgq-group rate-limit { <*kbit/s*> | <*Mbit/s*>M }

To delete information:

no shaper wgq-group rate-limit

Input mode

```
(config-if)
```

Parameters

rate-limit { <*kbit/s*> | <*Mbit/s*>M }

Specifies the WGQ bandwidth control value.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   - <*kbit/s*>: Specify 64 to 1000000.

   - <*Mbit/s*>: Specify 1 M to 1000 M.

3. Note on using this parameter:

   You cannot set a value that exceeds the port bandwidth control value.

Default behavior

WGQ bandwidth control is not set for the interface.

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 interface of a NIF that does not support the hierarchical shaper functionality.
2. If this command is set for an interface that is operating in a shaper mode other than the target shaper mode, the command is not applied to the device.

Related commands

shaper nif

traffic-shape rate

Sets the bandwidth by setting port bandwidth control for an interface (physical port) to limit the send bandwidth.

Syntax

To set or change information:

traffic-shape rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G}

To delete information:

no traffic-shape rate

Input mode

(config-if)

Parameters

rate {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G}

Sets port bandwidth control. Using this functionality limits the total-line send bandwidth to the set bandwidth.

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 (default), M, or G for the unit of the value.

   Set the bandwidth so that it is equal to or smaller than the line speed.

Table 7-24: Setting range for port bandwidth control

#	Line speed (including auto-negotiation results)	Setting range		Increment
1	10 Gbit/s	In Gbit/s	1 G to 10 G	1 Gbit/s
		In Mbit/s	100 M to 10000 M	100 Mbit/s
		In kbit/s	Not applicable	--
2	1 Gbit/s	In Gbit/s	1 G	--
		In Mbit/s	10 M to 1000 M	10 Mbit/s
		In kbit/s	Not applicable	--
3	100 Mbit/s	In Gbit/s	Not applicable	--
		In Mbit/s	1 M to 100 M	1 Mbit/s
		In kbit/s	Not applicable	--
4	10 Mbit/s#	In Gbit/s	Not applicable	--
		In Mbit/s	1 M to 10 M	1 Mbit/s
		In kbit/s	300 to 10000	100 kbit/s

Legend: --: Not applicable

#: Port bandwidth control works only in the full-duplex mode.

Default behavior

The send bandwidth is not limited.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Port bandwidth control does not work when the line status is half duplex.
2. When the set bandwidth for port bandwidth control exceeds the line speed, the port bandwidth is not controlled.
3. On a port for which port bandwidth control has been set, if the line speed is determined by auto-negotiation, port bandwidth control might not be able to work at the set bandwidth. In such a case, an operation log message is output.

   The following are examples in which port bandwidth control does not work:

   - When the bandwidth set for port bandwidth control exceeds the line speed determined by auto-negotiation

     (For example, the port bandwith is set to 50 Mbit/s, and the line speed is determined to be 1000 Mbit/s.)

   - When the unit for the bandwidth set for port bandwidth control is different from the unit set for the line speed determined by auto-negotiation

     (For example, the port bandwith is set to 50 Mbit/s, and the line speed is determined to be 1000 Mbit/s.)
4. This command cannot be set for an interface of a NIF that does not support the legacy shaper functionality.
5. This command cannot be set for an interface of a NIF for which the hierarchical shaper functionality has been set.

Related commands

interface gigabitethernet

interface tengigabitethernet

upc-storm-control mode

Sets the modes for bandwidth monitoring of the QoS functionality and storm control. This command changes the number of the maximum entries for bandwidth monitoring of the QoS functionality and storm control that can be accommodated in the hardware table per device. By changing the mode according to the operating mode, you can use hardware resources by collecting them for use in the necessary functionality.

This command is used to set basic operating conditions for the hardware. Before you use this command to change conditions, you must delete bandwidth monitoring of the QoS functionality. You might need to delete storm control depending on the mode to change to. Accordingly, you must set this command during the first step of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set or change information:

upc-storm-control mode {upc-in-and-storm-control | upc-in-in} [AX6700S]

upc-storm-control mode {upc-in-and-storm-control | upc-in-in | upc-in-out} [AX6600S] [AX6300S]

Input mode

`(config)`

Parameters

{upc-in-and-storm-control | upc-in-in} [AX6700S]

{upc-in-and-storm-control | upc-in-in | upc-in-out} [AX6600S] [AX6300S]

Specifies the bandwidth monitoring storm control mode.

`upc-in-and-storm-control` is used to set the mode in which bandwidth monitoring is set on the receiving side, and maximum bandwidth control or minimum bandwidth monitoring can be used with storm control for a flow detection condition.

`upc-in-in` is used to set the mode in which bandwidth monitoring is set on the receiving side, and maximum bandwidth control and minimum bandwidth monitoring can be used for a flow detection condition.

For AX6300S series switches, `upc-in-out` is used to set the mode in which bandwidth monitoring is set on the receiving side and the sending side, and maximum bandwidth control or minimum bandwidth monitoring can be used for a flow detection condition.

For details about the bandwidth monitoring storm control mode, see *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

`upc-in-and-storm-control` is set at the initial startup.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For AX6700S series switches, `upc-in-in` cannot be set if storm control is set.
2. For AX6600S and AX6300S series switches, `upc-in-in` or `upc-in-out` cannot be set if storm control is set.
3. When you set `upc-in-out` for the bandwidth monitoring storm control mode, specify 1 for the number of running PSP units in the following commands: [AX6600S]
   - redundancy max-psp
   - schedule-power-control max-psp
   - adaptive-power-control max-psp

Related commands

ip qos-flow-group

ipv6 qos-flow-group

mac qos-flow-group

storm-control (global)

storm-control (interface)

Chapter 8. Layer 2 Authentication

Configuration command and applicable Layer 2 authentication types
authentication ip access-group

Configuration command and applicable Layer 2 authentication types

The following table shows the configuration command used in common for Layer 2 authentication and the applicable Layer 2 authentication types.

Table 8-1: Configuration command and applicable Layer 2 authentication types

Command name	Applicable Layer 2 authentication types		
	IEEE 802.1X#1	Web authentication#2	MAC-based authentication
authentication ip access-group	Y	Y	Y

Legend:

Y: The command can be set.

#1: For IEEE 802.1X, the command cannot be applied in single-terminal and multi-terminal modes of port-based authentication.

#2: For Web authentication, the command is applied in fixed and dynamic VLAN modes.

authentication ip access-group

For IP packets sent from an unauthenticated terminal to other terminals, only the packet types enabled by the specified IPv4 access list are forwarded to unauthenticated ports.

Syntax

To set or change information:

authentication ip access-group {<*access list number*> | <*access list name*>}

To delete information:

no authentication ip access-group {<*access list number*> | <*access list name*>}

Input mode

`(config)`

Parameters

{<*access list number*> | <*access list name*>}

Specifies the identifier of the IPv4 packet filter to be used to restrict output of packets to ports that are not subject to authentication.

By using this parameter, one IPv4 packet filter identifier can be specified per device.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*access list number*>, specify values from 100 to 199, or from 2000 to 2699 (in decimal).

   For <*access list name*>, specify a name that is 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

1. For an authentication IPv4 access list, only `permit` is applicable as the action, and the filter conditions are limited to the following:
   - The protocol name `tcp` or `udp`
   - Destination IPv4 address and mask
   - Destination port number
2. The packets that match the authentication IPv4 access list have low processing priority in the device. For example, if control packets used in routing protocols match the authentication IPv4 access list, those packets might be lost due to their low processing priority in the device, which can cause some routes to disappear from the routing table.

Therefore, make sure that you set the minimum restrictions necessary by setting appropriate conditions in the authentication IPv4 access list to be applied, such as specifying only the hosts that require communication before authentication.

Related commands

dot1x system-auth-control

mac-authentication system-auth-control

web-authentication system-auth-control

Chapter 9. IEEE802.1X

aaa accounting dot1x default
aaa authentication dot1x default
aaa authorization network default
dot1x force-authorized-port
dot1x ignore-eapol-start
dot1x logging enable
dot1x loglevel
dot1x max-req
dot1x max-supplicant
dot1x multiple-authentication
dot1x multiple-hosts
dot1x port-control
dot1x reauthentication
dot1x supplicant-detection
dot1x system-auth-control
dot1x timeout keep-unauth
dot1x timeout quiet-period
dot1x timeout reauth-period
dot1x timeout server-timeout
dot1x timeout supp-timeout
dot1x timeout tx-period
dot1x vlan dynamic enable
dot1x vlan dynamic ignore-eapol-start
dot1x vlan dynamic max-req
dot1x vlan dynamic max-supplicant
dot1x vlan dynamic radius-vlan
dot1x vlan dynamic reauthentication
dot1x vlan dynamic supplicant-detection
dot1x vlan dynamic timeout quiet-period
dot1x vlan dynamic timeout reauth-period
dot1x vlan dynamic timeout server-timeout
dot1x vlan dynamic timeout supp-timeout
dot1x vlan dynamic timeout tx-period
dot1x vlan enable
dot1x vlan ignore-eapol-start
dot1x vlan max-req
dot1x vlan max-supplicant
dot1x vlan reauthentication
dot1x vlan supplicant-detection
dot1x vlan timeout quiet-period
dot1x vlan timeout reauth-period
dot1x vlan timeout server-timeout
dot1x vlan timeout supp-timeout
dot1x vlan timeout tx-period

aaa accounting dot1x default

Enables the collection of accounting information on the use of the specified authentication method. Only accounting information for IEEE 802.1X authentication is collected.

Syntax

To set information:

aaa accounting dot1x default start-stop group radius

To delete information:

no aaa accounting dot1x default

Input mode

(config)

Parameters

start-stop

If authentication is successful, the accounting start notification is sent to the accounting server. If authentication is canceled, the accounting stop notification is sent to the accounting server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   start-stop

group radius

Requests accounting information for use of RADIUS server authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   group radius

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

dot1x system-auth-control

radius-server host

aaa authentication dot1x default

Specifies IEEE 802.1X user authentication.

Syntax

To set information:

aaa authentication dot1x default group radius

To delete information:

no aaa authentication dot1x default

Input mode

(config)

Parameters

group radius

IEEE 802.1X authentication is performed by a RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   group radius

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 this command is not set, the RADIUS server cannot be used for IEEE 802.1X authentication.

Related commands

aaa authorization network

dot1x system-auth-control

radius-server host

aaa authorization network default

Specify this command to perform per-VLAN VLAN-based authentication (dynamic) using the specified authentication method.

Syntax

To set information:

aaa authorization network default group radius

To delete information:

no aaa authorization network default

Input mode

(config)

Parameters

group radius

IEEE 802.1X authentication is performed by a RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   group radius

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 this command is not set, VLAN-based authentication (dynamic) cannot be used.

Related commands

dot1x vlan dynamic enable

aaa authentication dot1x

radius-server host

dot1x force-authorized-port

In a VLAN configured for per-VLAN VLAN-based authentication (static), sets a specific port or channel group for which communication is allowed without the need for authentication.

Syntax

To set information:

dot1x force-authorized-port

To delete information:

no dot1x force-authorized-port

Input mode

`(config-if)`

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

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. Do not set this command for a port that uses Web authentication or MAC-based authentication.

Related commands

dot1x system-auth-control

dot1x vlan enable

dot1x ignore-eapol-start

Sets the Switch not to issue EAP-Request/Identity packets in response to EAPOL-Start from a supplicant.

Syntax

To set information:

dot1x ignore-eapol-start

To delete information:

no dot1x ignore-eapol-start

Input mode

`(config-if)`

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

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. This command can be set only on an interface for which both the `dot1x reauthentication` command and the `dot1x supplicant-detection` command (without the `disable` parameter) have been set.
4. This command cannot be set for an interface for which the `dot1x supplicant-detection` command with the `disable` parameter has been set.
5. For an interface for which this command has been set, you cannot use the `no dot1x reauthentication` command to set no re-authentication.

Related commands

dot1x reauthentication

dot1x supplicant-detection

dot1x system-auth-control

dot1x port-control

dot1x logging enable

For IEEE 802.1X authentication, enables operation log information to be output to a syslog server.

Syntax

To set information:

dot1x logging enable

To delete information:

no dot1x logging enable

Input mode

(config)

Parameters

None

Default behavior

Operation log information is not output to a syslog server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

dot1x loglevel

dot1x system-auth-control

logging email-event-kind

logging event-kind

dot1x loglevel

Specifies the level of messages to be logged in an IEEE 802.1X operation log. Use the `show dot1x logging` operation command to display the logged messages.

Syntax

To set or change information:

dot1x loglevel {error | warning | notice | info}

To delete information:

no dot1x loglevel

Input mode

`(config)`

Parameters

{error | warning | notice | info}

error

Only error-level log messages are logged. Only software errors are logged.

warning

Error-level and warning-level messages are logged. Detected error information, such as information about invalid frames, is logged.

notice

error-, warning-, notice-, and normal-level messages are logged. Information on whether authentication is supported, and information on server connectivity is logged.

info

error-, warning-, notice-, normal-, and info-level messages are logged. Operation tracking information is also logged.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `error`, `warning`, `notice`, or `info`

Default behavior

The level of messages logged in the operation log is `info`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.

Related commands

dot1x system-auth-control

dot1x max-req

Specifies the maximum number of EAP-Request retransmissions if the supp-timeout value is exceeded. If the number of retransmissions exceeds this value, authentication is determined to have failed.

Syntax

To set or change information:

dot1x max-req <*count*>

To delete information:

no dot1x max-req

Input mode

```
(config-if)
```

Parameters

<*count*>

Specifies the maximum number of EAP-Request retransmissions.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of EAP-Request retransmissions is two.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.

Related commands

dot1x system-auth-control

dot1x timeout supp-timeout

dot1x port-control

dot1x max-supplicant

Specifies the maximum number of terminals that can be connected to the specified interface when terminal authentication submode is set. If more terminals than this value attempt to connect, the number of terminals that can connect is restricted without attempting authentication.

Syntax

To set or change information:

dot1x max-supplicant <*clients*>

To delete information:

no dot1x max-supplicant

Input mode

`(config-if)`

Parameters

<*clients*>

Specifies the maximum number of terminals that can connect to the specified interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 256

Default behavior

The maximum number of terminals that can be connected is 256.

Impact on communication

If the specified value is smaller than the number of terminals that are currently authenticated on the specified interface, the authentication status of all supplicants that are currently authenticated on the specified interface is canceled. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. If the specified value is smaller than the number of terminals that are currently authenticated on the specified interface, the authentication status of all supplicants that are authenticated on the specified interface is temporarily canceled.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x multiple-authentication

Sets the IEEE 802.1X authentication submode to terminal authentication mode. The command performs authentication for each terminal and the authentication result determines whether communication is possible. Accordingly, multiple terminals can be connected. For a terminal configured by the `mac-address-table static` command, communication is always possible regardless of the authentication status if `auto` is set for the `dot1x port-control` command.

If multi-terminal or terminal authentication submodes are not set, single mode is used. Single mode authentication permits connection of only one terminal. When multiple terminals are connected, the status of the specified interface changes to not authenticated. For a terminal configured by the `mac-address-table static` command, communication is not possible until terminal authentication is successful.

Syntax

To set information:

dot1x multiple-authentication

To delete information:

no dot1x multiple-authentication

Input mode

`(config-if)`

Parameters

None

Default behavior

The authentication submode is single mode.

Impact on communication

If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate.
4. If the `dot1x multiple-hosts` or `dot1x multiple-authentication` commands are not set, the single authentication submode is used.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x multiple-hosts

dot1x multiple-hosts

Sets IEEE 802.1X authentication with a multi-terminal submode. Initially, only the terminal that starts authentication first is subject to authentication. After this authentication is successful, other terminals can communicate without needing to authenticate. Accordingly, multiple terminals can be connected. For a terminal configured by the `mac-address-table static` command, communication is not possible until terminal authentication is successful.

If multi-terminal or terminal authentication submodes are not set, single mode is used. Single mode authentication permits connection of only one terminal. When multiple terminals are connected, the status of the specified interface changes to not authenticated. For a terminal configured by the `mac-address-table static` command, communication is not possible until terminal authentication is successful.

Syntax

To set information:

dot1x multiple-hosts

To delete information:

no dot1x multiple-hosts

Input mode

`(config-if)`

Parameters

None

Default behavior

The authentication submode is single mode.

Impact on communication

If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate.
4. If the `dot1x multiple-hosts` or `dot1x multiple-authentication` commands are not set, the single authentication submode is used.
5. Do not set this command for a port that uses Web authentication or MAC-based authentication.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x multiple-authentication

dot1x port-control

Sets the port-control status for a specified interface. Entering this command also enables the IEEE 802.1X port-based authentication functionality.

Syntax

To set or change information:

dot1x port-control {auto | force-authorized | force-unauthorized}

To delete information:

no dot1x port-control

Input mode

(config-if)

Parameters

{auto | force-authorized | force-unauthorized}

auto

IEEE 802.1X authentication is performed. The authentication result determines whether communication is enabled for terminals connected to the interface.

force-authorized

IEEE 802.1X authentication is not performed, and communication by terminals connected to the specified interface is always possible.

force-unauthorized

IEEE 802.1X authentication is not performed, and communication by terminals connected to the specified interface is never possible.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   auto, force-authorized, or force-unauthorized

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the dot1x system-auth-control command is set.
2. If the dot1x multiple-hosts or dot1x multiple-authentication commands have not been set, the authentication submode is single mode.
3. This command cannot be set for interfaces that belong to VLANs with VLAN-based authentication.
4. This command cannot be set for interfaces whose access modes have not been set.

5. This command cannot be set for a tunneling port.
6. This command cannot be set for interfaces belonging to a VLAN with MAC address learning suppression.
7. This command cannot be set for interfaces where MAC address learning count restriction is set.
8. This command cannot be set for interfaces belonging to a VLAN where MAC address learning count restriction is set.
9. This command cannot be set for interfaces belonging to a VLAN where EAPOL forwarding functionality is specified.
10. Do not set the `dot1x port-control force-authorized` or `dot1x port-control force-unauthorized` command for an authentication port for Web authentication or MAC-based authentication.
11. If you set this command for an authentication port for Web authentication or MAC-based authentication, set the authentication submode to terminal authentication.

Related commands

dot1x system-auth-control

dot1x multiple-hosts

dot1x multiple-authentication

dot1x vlan enable

switchport mode

switchport access

dot1x reauthentication

After successful IEEE 802.1X authentication, this command sets whether a supplicant is to be re-authenticated. When this command is in effect, `EAP-Request/Identity` packets for re-authentication are sent at the interval set by using the `dot1x timeout reauth-period` command to a supplicant as a prompt for supplicant re-authentication.

Syntax

To set information:

dot1x reauthentication

To delete information:

no dot1x reauthentication

Input mode

`(config-if)`

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

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. For an interface for which the `dot1x ignore-eapol-start` command has been specified, you cannot use the `no dot1x reauthentication` command to set no re-authentication.

Related commands

dot1x ignore-eapol-start

dot1x timeout reauth-period

dot1x system-auth-control

dot1x port-control

dot1x supplicant-detection

Specifies the behavior when a new terminal is detected after terminal authentication submode has been specified for authentication.

Syntax

To set or change information:

dot1x supplicant-detection {disable | shortcut}

To delete information:

dot1x supplicant-detection

Input mode

(config-if)

Parameters

{disable | shortcut}

Specifies the behavior when a new terminal is detected after terminal authentication submode has been set for authentication.

disable

If terminal authentication submode is set, and there are authenticated terminals, this suppresses EAP-Request/Identity transmission for detecting a new terminal. Specify this parameter if a supplicant operates abnormally if the authentication sequence is omitted in order to decrease switch load.

If this parameter is specified, even a supplicant that is unable to initiate authentication from a terminal can have EAP-Request/Identity packets sent in response to the data frame from the terminal in order to start authentication.

shortcut

If terminal authentication submode is set, when detecting new terminals this parameter causes the authentication sequence for already-authenticated terminals to be skipped to reduce the load on the Switch during EAP-Request/Identity transmission. Specify this parameter for a supplicant that is unable to initiate authentication from a terminal.

If this parameter is specified, some supplicants might not operate correctly and communication is temporarily stopped.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   disable or shortcut

Default behavior

shortcut is used as the operation when a new terminal is detected.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. The `dot1x supplicant-detection` command is valid only if the `dot1x multiple-authentication` command has been set.
4. `disable` cannot be set for the `dot1x supplicant-detection` command on an interface for which the `dot1x ignore-eapol-start` command has been set.

Related commands

dot1x ignore-eapol-start

dot1x multiple-authentication

dot1x system-auth-control

dot1x port-control

dot1x system-auth-control

Enables IEEE 802.1X.

Syntax

To set information:

dot1x system-auth-control

To delete information:

no dot1x system-auth-control

Input mode

(config)

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

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. If an authentication VLAN configuration has been set, this command fails and IEEE 802.1X is not enabled.
3. If GSRP has been set, this command fails and IEEE 802.1X is not enabled.
4. If the `aaa authentication dot1x default group radius` command has not been set, a RADIUS server cannot be used for IEEE 802.1X authentication.

Related commands

aaa authentication dot1x default

dot1x timeout keep-unauth

Specifies the period of time (in seconds) for maintaining the communication-disabled state of the interface if two or more terminals are connected to an interface on which the single-mode authentication submode is set. After the time set by using this command elapses, an authenticated terminal must be re-authenticated.

Syntax

To set or change information:

dot1x timeout keep-unauth <*seconds*>

To delete information:

no dot1x timeout keep-unauth

Input mode

`(config-if)`

Parameters

<*seconds*>

Specifies the period of time (in seconds) for maintaining communication-disabled state when single authentication submode is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

3600 seconds is used as the period of time for maintaining the communication-disabled state.

Impact on communication

None

When the change is applied

When the communication becomes impossible.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. The value set for this command is applied only to an interface in single-mode authentication submode.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x multiple-hosts

dot1x multiple-authentication

dot1x timeout quiet-period

Specifies the period of time (in seconds) for maintaining the unauthenticated state on the applicable interface after an IEEE 802.1X authentication failure. During this period, no EAPOL packets are sent and received EAPOL packets are ignored. Also, no authentication is performed.

Syntax

To set or change information:

dot1x timeout quiet-period <*seconds*>

To delete information:

no dot1x timeout quiet-period

Input mode

`(config-if)`

Parameters

<*seconds*>

Specifies the period of time (in seconds) for maintaining the unauthenticated state.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

60 seconds is used as the period for maintaining the unauthenticated state.

Impact on communication

None

When the change is applied

When the Switch enters an unauthenticated state due to an authentication failure.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x timeout reauth-period

Specifies the interval (in seconds) for re-authenticating a supplicant after a successful IEEE 802.1X authentication. EAP-Request/Identify packets for re-authentication are sent to the supplicant at the interval set by using this command as a prompt for supplicant re-authentication.

Syntax

To set or change information:

dot1x timeout reauth-period <*seconds*>

To delete information:

no dot1x timeout reauth-period

Input mode

`(config-if)`

Parameters

<*seconds*>

Specifies the interval (in seconds) for re-authenticating a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

3600 seconds is used as the interval for re-authenticating a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.
- When a terminal is authenticated successfully at the authentication level when there are no authenticated terminals.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. This command takes effect only if re-authentication has been set by using the `dot1x reauthentication` command.
4. For the parameter, set a value greater than the value set by using the `dot1x timeout tx-period` command.

Related commands

dot1x timeout tx-period

dot1x reauthentication

dot1x system-auth-control

dot1x port-control

dot1x timeout server-timeout

Specifies the time (in seconds) to wait for a response, including the time required for retransmitting a response to an authentication server.

Syntax

To set or change information:

dot1x timeout server-timeout <*seconds*>

To delete information:

no dot1x timeout server-timeout

Input mode

`(config-if)`

Parameters

<*seconds*>

Specifies the time (in seconds) to wait for a response.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x timeout supp-timeout

Specifies the time (in seconds) to wait for a response from a supplicant for an EAP-Request packet sent to a supplicant. If no response is received during the specified period, the EAP-Request packet is retransmitted.

Syntax

To set or change information:

dot1x timeout supp-timeout <*seconds*>

To delete information:

no dot1x timeout supp-timeout

Input mode

`(config-if)`

Parameters

<*seconds*>

Specifies the time (in seconds) to wait for a response from a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response from a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.

Related commands

dot1x system-auth-control

dot1x max-req

dot1x port-control

dot1x timeout tx-period

Specifies the interval (in seconds) for sending EAP-Request/Identity packets when IEEE 802.1X is valid.

Syntax

To set or change information:

dot1x timeout tx-period <*seconds*>

To delete information:

no dot1x timeout tx-period

Input mode

`(config-if)`

Parameters

<*seconds*>

Specifies the interval (in seconds) for sending EAP-Request/Identity packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the interval for sending EAP-Request/Identity packets.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x port-control` command has been set.
3. Specify a value smaller than the one set by using the `dot1x timeout reauth-period` command as the parameter value.

Related commands

dot1x timeout reauth-period

dot1x system-auth-control

dot1x port-control

dot1x vlan dynamic enable

Enables IEEE 802.1X VLAN-based authentication (dynamic).

Syntax

To set information:

dot1x vlan dynamic enable

To delete information:

no dot1x vlan dynamic enable

Input mode

`(config)`

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

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. When you set the `dot1x vlan dynamic enable` command, it will take effect only if you also set the `aaa authorization network default group radius` command.
3. When the `dot1x vlan dynamic enable` command has not been set, none of the VLAN-based authentication (dynamic) functionality is enabled.

Related commands

dot1x system-auth-control

aaa authorization network default

dot1x vlan dynamic ignore-eapol-start

Sets the Switch not to issue EAP-Request/Identity packets in response to EAPOL-Start from a supplicant.

Syntax

To set information:

dot1x vlan dynamic ignore-eapol-start

To delete information:

no dot1x vlan dynamic ignore-eapol-start

Input mode

`(config)`

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

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.
3. This command can be set only on an interface on which the `dot1x vlan dynamic reauthentication` command is set and `disable` is not specified in the `dot1x vlan dynamic supplicant-detection` command.
4. This command cannot be set on an interface for which `disable` is specified in the `dot1x vlan dynamic supplicant-detection` command.
5. For an interface for which this command has been set, you cannot use the `no dot1x vlan dynamic reauthentication` command to set no re-authentication.

Related commands

dot1x vlan dynamic reauthentication

dot1x vlan dynamic supplicant-detection

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic max-req

Specifies the maximum number of EAP-Request retransmissions if the supp-timeout value is exceeded. If the number of retransmissions exceeds this value, authentication is determined to have failed.

Syntax

To set or change information:

dot1x vlan dynamic max-req <*count*>

To delete information:

no dot1x vlan dynamic max-req

Input mode

`(config)`

Parameters

<*count*>

Specifies the maximum number of EAP-Request retransmissions.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of EAP-Request retransmissions is two.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan dynamic timeout supp-timeout

dot1x vlan dynamic enable

dot1x vlan dynamic max-supplicant

Specifies the maximum number of terminals that can be connected for VLAN-based authentication (dynamic). If more terminals than this value attempt to connect, the number of terminals that can connect is restricted without attempting authentication.

Syntax

To set or change information:

dot1x vlan dynamic max-supplicant <*clients*>

To delete information:

no dot1x vlan dynamic max-supplicant

Input mode

`(config)`

Parameters

<*clients*>

Specifies the maximum number of terminals that can be connected for VLAN-based authentication (dynamic).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4096

Default behavior

The maximum number of terminals is 4096.

Impact on communication

If the specified value is smaller than the number of terminals that are currently authenticated on the specified interface, the authentication status of all supplicants that are currently authenticated on the specified interface is canceled. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.
3. If the specified value is smaller than the number of terminals that are currently authenticated by VLAN-based authentication (dynamic), authentication status of all supplicants that are authenticated by VLAN-based authentication (dynamic) is canceled.

Related commands

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic radius-vlan

Specifies VLANs to allow dynamic VLAN allocation according to VLAN information sent from the RADIUS server during IEEE 802.1X authentication.

Syntax

To set information:

dot1x vlan dynamic radius-vlan <*vlan id list*>

To change information:

dot1x vlan dynamic radius-vlan {<*vlan id list*> | add <*vlan id list*> | remove <*vlan id list*>}

To delete information:

no dot1x vlan dynamic radius-vlan

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. Changing the parameter replaces the existing VLANs with the VLANs that have been specified. The specifiable VLANs are MAC VLANs only.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

add <*vlan id list*>

Specifies VLANs to be added to the VLANs to which the IEEE 802.1X authentication settings are applied. The specifiable VLANs are MAC VLANs only.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

remove <*vlan id list*>

Specifies VLANs to be removed from the VLANs to which the IEEE 802.1X authentication settings are applied. The specifiable VLANs are MAC VLANs only.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified

for this 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. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.
3. The sum of VLANs with dynamic and static VLAN-based authentication can be no more than 1024.
4. The sum of the ports and channel groups belonging to any of the VLANs having a configuration of dynamic or static VLAN-based authentication can be no more than 1024. VLANs cannot be specified if the sum exceeds the upper limit.
5. If none of the VLANs that fall within the range can be set, an error occurs.
6. A VLAN for which MAC address learning suppression is set cannot be specified.
7. A VLAN for which MAC address learning count restriction is set cannot be specified.
8. A VLAN to which an interface where MAC address learning count restriction is set belongs cannot be specified.
9. A VLAN for which EAPOL forwarding functionality is set cannot be specified.

Related commands

vlan

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan enable

switchport mac

dot1x vlan dynamic reauthentication

After successful IEEE 802.1X authentication, this command sets whether a supplicant is to be re-authenticated. When this command is in effect, EAP-Request/Identity packets for re-authentication are sent to a supplicant at the interval set by using the `dot1x vlan dynamic timeout reauth-period` command as a prompt for supplicant re-authentication.

Syntax

To set information:

dot1x vlan dynamic reauthentication

To delete information:

no dot1x vlan dynamic reauthentication

Input mode

`(config)`

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

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.
3. For an interface for which the `dot1x vlan dynamic ignore-eapol-start` command has been specified, you cannot use the `no dot1x vlan dynamic reauthentication` command to set no re-authentication.

Related commands

dot1x system-auth-control

dot1x vlan dynamic ignore-eapol-start

dot1x vlan dynamic timeout reauth-period

dot1x vlan dynamic enable

dot1x vlan dynamic supplicant-detection

Specifies the behavior when a new terminal is detected.

Syntax

To set or change information:

dot1x vlan dynamic supplicant-detection {disable | shortcut}

To delete information:

no dot1x vlan dynamic supplicant-detection

Input mode

(config)

Parameters

{disable | shortcut}

Specifies the behavior when a new terminal is detected.

disable

If terminal authentication submode is set, and there are authenticated terminals, this suppresses EAP-Request/Identity transmission for detecting a new terminal. Specify this parameter if a supplicant operates abnormally if the authentication sequence is omitted in order to decrease switch load.

If this parameter is specified, even a supplicant that is unable to initiate authentication from a terminal can have EAP-Request/Identity packets sent in response to the data frame from the terminal in order to start authentication.

shortcut

Omits the authentication sequence of an authenticated terminal during EAP-Request/Identity transmission for detecting a new terminal to reduce the load. Specify this parameter for a supplicant that is unable to initiate authentication from a terminal.

If this parameter is specified, some supplicants might not operate correctly, and communication is temporarily stopped.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   disable or shortcut

Default behavior

shortcut is used as the operation when a new terminal is detected.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the dot1x system-auth-control command is set.
2. This command takes effect only if the dot1x vlan dynamic enable command has been set.

3. On the interface on which the `dot1x vlan dynamic ignore-eapol-start` command is specified, `disable` cannot be set for the `dot1x vlan dynamic supplicant-detection` command.

Related commands

dot1x vlan dynamic ignore-eapol-start

dot1x vlan dynamic enable

dot1x system-auth-control

dot1x vlan dynamic timeout quiet-period

Specifies the period of time (in seconds) for maintaining the unauthenticated state on the applicable interface after an IEEE 802.1X authentication failure. During this period, no EAPOL packets are sent and received EAPOL packets are ignored. Also, no authentication is performed.

Syntax

To set or change information:

dot1x vlan dynamic timeout quiet-period <*seconds*>

To delete information:

no dot1x vlan dynamic timeout quiet-period

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the period of time (in seconds) for maintaining the unauthenticated state.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

60 seconds is used as the period for maintaining the unauthenticated state.

Impact on communication

None

When the change is applied

When the Switch enters the unauthenticated state due to an authentication failure.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout reauth-period

Specifies the interval (in seconds) for re-authenticating a supplicant after a successful IEEE 802.1X authentication. EAP-Request/Identify packets for re-authentication are sent to the supplicant at the interval set by using this command as a prompt for supplicant re-authentication.

Syntax

To set or change information:

dot1x vlan dynamic timeout reauth-period <*seconds*>

To delete information:

no dot1x vlan dynamic timeout reauth-period

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the interval (in seconds) for re-authenticating a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

3600 seconds is used as the interval for re-authenticating a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.
- When a terminal is authenticated successfully at the authentication level when there are no authenticated terminals.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.
3. This command takes effect only if re-authentication has been set by using the `dot1x vlan dynamic reauthentication` command.
4. For the parameter, a value greater than the value set by using the `dot1x vlan dynamic timeout tx-period` command.

Related commands

dot1x vlan dynamic timeout tx-period

dot1x vlan dynamic reauthentication

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout server-timeout

Specifies the time (in seconds) to wait for a response, including the time required for retransmitting a response to an authentication server.

Syntax

To set or change information:

dot1x vlan dynamic timeout server-timeout <*seconds*>

To delete information:

no dot1x vlan dynamic timeout server-timeout

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the time (in seconds) to wait for a response.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan dynamic enable

dot1x vlan dynamic timeout supp-timeout

Specifies the time (in seconds) to wait for a response from a supplicant for an EAP-Request packet sent to a supplicant. If no response is received during the specified period, the EAP-Request packet is retransmitted.

Syntax

To set or change information:

dot1x vlan dynamic timeout supp-timeout <*seconds*>

To delete information:

no dot1x vlan dynamic timeout supp-timeout

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the time (in seconds) to wait for a response from a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response from a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan dynamic max-req

dot1x vlan dynamic enable

dot1x vlan dynamic timeout tx-period

Specifies the interval (in seconds) for sending EAP-Request/Identity packets when IEEE 802.1X authentication is valid.

Syntax

To set or change information:

dot1x vlan dynamic timeout tx-period <*seconds*>

To delete information:

no dot1x vlan dynamic timeout tx-period

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the interval (in seconds) for sending EAP-Request/Identity packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the interval for sending EAP-Request/Identity packets.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan dynamic enable` command has been set.
3. For the parameter, set a value smaller than the value set by using the `dot1x vlan dynamic timeout reauth-period` command.

Related commands

dot1x system-auth-control

dot1x vlan dynamic timeout reauth-period

dot1x vlan dynamic enable

dot1x vlan enable

Enables IEEE 802.1X VLAN-based authentication (static).

Syntax

To set information:

dot1x vlan <*vlan id list*> enable

To delete information:

no dot1x vlan <*vlan id list*> enable

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this 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. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. If this command is not set, VLAN-based authentication (static) cannot be used.
3. If none of the VLANs that fall within the range can be set, an error occurs.
4. VLAN-based authentication (static) is not available in VLANs that include ports or channel group ports that have a port-based authentication configuration.
5. The sum of VLANs with dynamic and static VLAN-based authentication can be no more than 1024.
6. The sum of the ports and channel groups belonging to any of the VLANs having a configuration of dynamic or static VLAN-based authentication can be no more than 1024. VLANs cannot be specified if the sum exceeds the upper limit.
7. VLAN-based authentication (static) is not available for a native VLAN of MAC ports or protocol ports.
8. A VLAN to which a tunneling port belongs cannot be specified.

9. A VLAN for which MAC address learning suppression is set cannot be specified.
10. A VLAN for which MAC address learning count restriction is set cannot be specified.
11. A VLAN to which an interface where MAC address learning count restriction is set belongs cannot be specified.
12. A VLAN for which EAPOL forwarding functionality is set cannot be specified.

Related commands

vlan

dot1x system-auth-control

dot1x port-control

dot1x vlan dynamic radius-vlan

switchport mode

switchport access

dot1x vlan ignore-eapol-start

Sets the Switch not to issue EAP-Request/Identity packets in response to EAPOL-Start from a supplicant.

Syntax

To set information:

dot1x vlan <*vlan id list*> ignore-eapol-start

To delete information:

no dot1x vlan <*vlan id list*> ignore-eapol-start

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this 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. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.
3. This command can be set only on an interface on which the `dot1x vlan` <*vlan id list*> `reauthentication` command is set and `disable` is not set for the `dot1x vlan` <*vlan id list*> `supplicant-detection` command.
4. This command cannot be set on an interface on which the `dot1x vlan` <*vlan id list*> `supplicant-detection` command has been set with the `disable` parameter specified.
5. For an interface for which this command has been set, you cannot use the `no dot1x vlan` <*vlan id list*> `reauthentication` command to set no re-authentication.

Related commands

dot1x vlan reauthentication

dot1x vlan supplicant-detection

dot1x system-auth-control

dot1x vlan enable

dot1x vlan max-req

Specifies the maximum number of EAP-Request retransmissions if the supp-timeout value is exceeded. If the number of retransmissions exceeds this value, authentication is determined to have failed.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> max-req <*count*>

To delete information:

no dot1x vlan <*vlan id list*> max-req

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

<*count*>

Specifies the maximum number of EAP-Request retransmissions.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of EAP-Request retransmissions is two.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan timeout supp-timeout

dot1x vlan enable

dot1x vlan max-supplicant

Specifies the maximum number of terminals that can be connected to the specified VLAN interface. If more terminals than this value attempt to connect, the number of terminals that can connect is restricted without attempting authentication.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> max-supplicant <*clients*>

To delete information:

no dot1x vlan <*vlan id list*> max-supplicant

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

<*clients*>

Specifies the maximum number of terminals that can be connected to the specified VLAN interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 256

Default behavior

The number of terminals that can be connected is 256.

Impact on communication

If the specified value is smaller than the number of terminals that are currently authenticated on the specified interface, the authentication status of all supplicants that are currently authenticated on the specified interface is canceled. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.

2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.
3. If the specified value is smaller than the number of terminals that are currently authenticated by VLAN-based authentication (static), authentication status of all supplicants that are authenticated by VLAN-based authentication (static) is canceled.

Related commands

dot1x system-auth-control

dot1x vlan enable

dot1x vlan reauthentication

After successful IEEE 802.1X authentication, this command sets whether a supplicant is to be re-authenticated. When this command is in effect, EAP-Request/Identity packets for re-authentication are sent to a supplicant at the interval set by using the `dot1x vlan` <*vlan id list*> `timeout reauth-period` command as a prompt for supplicant re-authentication.

Syntax

To set information:

dot1x vlan <*vlan id list*> reauthentication

To delete information:

no dot1x vlan <*vlan id list*> reauthentication

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this 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. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.
3. For a VLAN interface for which the `dot1x vlan` <*vlan id list*> `ignore-eapol-start` command has been specified, you cannot use the `no dot1x vlan` <*vlan id list*> `reauthentication` command to set no re-authentication.

Related commands

dot1x system-auth-control

dot1x vlan ignore-eapol-start

dot1x vlan timeout reauth-period

dot1x vlan enable

dot1x vlan supplicant-detection

Specifies the behavior when a new terminal is detected.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> supplicant-detection {disable | shortcut}

To delete information:

no dot1x vlan <*vlan id list*> supplicant-detection

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

{disable | shortcut}

Specifies the behavior when a new terminal is detected.

disable

If terminal authentication submode is set, and there are authenticated terminals, this suppresses EAP-Request/Identity transmission for detecting a new terminal. Specify this parameter if a supplicant operates abnormally if the authentication sequence is omitted in order to decrease switch load.

If this parameter is specified, even a supplicant that is unable to initiate authentication from a terminal can have EAP-Request/Identity packets sent in response to the data frame from the terminal in order to start authentication.

shortcut

Omits the authentication sequence of an authenticated terminal during EAP-Request/Identity transmission for detecting a new terminal to reduce the load. Specify this parameter for a supplicant that is unable to initiate authentication from a terminal.

If this parameter is specified, some supplicants might not operate correctly, and communication is temporarily stopped.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `disable` or `shortcut`

Default behavior

`shortcut` is used as the operation when a new terminal is detected.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.
3. On the interface on which the `dot1x vlan` <*vlan id list*> `ignore-eapol-start` command is specified, `disable` cannot be set for the `dot1x vlan` <*vlan id list*> `supplicant-detection` command.

Related commands

dot1x vlan ignore-eapol-start

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout quiet-period

Specifies the period of time (in seconds) for maintaining the unauthenticated state on the applicable VLAN interface after an IEEE 802.1X authentication failure. During this period, no EAPOL packets are sent and received EAPOL packets are ignored. Also, no authentication is performed.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> timeout quiet-period <*seconds*>

To delete information:

no dot1x vlan <*vlan id list*> timeout quiet-period

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

<*seconds*>

Specifies the period of time (in seconds) for maintaining the unauthenticated state.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

60 seconds is used as the period for maintaining the unauthenticated state.

Impact on communication

None

When the change is applied

When the Switch enters an unauthenticated state due to an authentication failure.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout reauth-period

Specifies the interval (in seconds) for re-authenticating a supplicant after a successful IEEE 802.1X authentication. EAP-Request/Identify packets for re-authentication are sent to the supplicant at the interval set by using this command as a prompt for supplicant re-authentication.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> timeout reauth-period <*seconds*>

To delete information:

no dot1x vlan <*vlan id list*> timeout reauth-period

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

<*seconds*>

Specifies the interval (in seconds) for re-authenticating a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

3600 seconds is used as the interval for re-authenticating a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.
- When a terminal is authenticated successfully at the authentication level when there are no authenticated terminals.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.
3. This command takes effect only if re-authentication has been set by using the `dot1x vlan` <*vlan id list*> `reauthentication` command.
4. For the parameter, set a value greater than the value set by using the `dot1x vlan` <*vlan id list*> `timeout tx-period` command.

Related commands

dot1x vlan timeout tx-period

dot1x vlan reauthentication

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout server-timeout

Specifies the time (in seconds) to wait for a response, including the time required for retransmitting a response to an authentication server.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> timeout server-timeout <*seconds*>

To delete information:

no dot1x vlan <*vlan id list*> timeout server-timeout

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

<*seconds*>

Specifies the time (in seconds) to wait for a response.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan enable

dot1x vlan timeout supp-timeout

Specifies the time (in seconds) to wait for a response from a supplicant for an EAP-Request packet sent to a supplicant. If no response is received during the specified period, the EAP-Request packet is retransmitted.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> timeout supp-timeout <*seconds*>

To delete information:

no dot1x vlan <*vlan id list*> timeout supp-timeout

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

<*seconds*>

Specifies the time (in seconds) to wait for a response from a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response from a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.

Related commands

dot1x system-auth-control

dot1x vlan max-req

dot1x vlan enable

dot1x vlan timeout tx-period

Specifies the interval (in seconds) for sending EAP-Request/Identity packets when IEEE 802.1X is valid.

Syntax

To set or change information:

dot1x vlan <*vlan id list*> timeout tx-period <*seconds*>

To delete information:

no dot1x vlan <*vlan id list*> timeout tx-period

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the IDs of VLANs to which the IEEE 802.1X authentication settings are applied. VLANs that have not been set for the Switch cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

<*seconds*>

Specifies the interval (in seconds) for sending EAP-Request/Identity packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the interval for sending EAP-Request/Identity packets.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. This command takes effect only if the `dot1x vlan` <*vlan id list*> `enable` command has been set.

3. For the parameter, set a value smaller than the value set by using the `dot1x vlan` <*vlan id list*> `timeout reauth-period` command.

Related commands

dot1x vlan timeout reauth-period

dot1x system-auth-control

dot1x vlan enable

Chapter

10. Web Authentication

Correspondence between configuration commands and operation modes

The following table describes the Web authentication operation modes in which Web authentication configuration commands can be set.

Table 10-1: Configuration commands and Web authentication operation modes

Command name	Web authentication operation modes		
	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode
aaa accounting web-authentication default start-stop group radius	Y	Y	Y
aaa authentication web-authentication default group radius	Y	Y	Y
authentication ip access-group	Y	Y	--
web-authentication auto-logout	--	Y	Y
web-authentication ip address	Y	Y	--
web-authentication jump-url	Y	Y	Y
web-authentication logging enable	Y	Y	Y
web-authentication logout ping tos-windows	Y	--	--
web-authentication logout ping ttl	Y	--	--
web-authentication logout polling count	Y	--	--
web-authentication logout polling enable	Y	--	--
web-authentication logout polling interval	Y	--	--
web-authentication logout polling retry-interval	Y	--	--
web-authentication max-timer	Y	Y	Y
web-authentication max-user	--	Y	Y
web-authentication port	Y	Y	N
web-authentication redirect-mode	--	Y	--
web-authentication redirect-vlan	--	Y	--
web-authentication static-vlan max-user	Y	--	--
web-authentication system-auth-control	Y	Y	Y
web-authentication vlan	N	N	Y
web-authentication web-port	Y	Y	Y

Legend:

Y: The command can be set, and the setting is applied.

--: The command can be set, but the setting is not applied.
N: The command cannot be set.

aaa accounting web-authentication default start-stop group radius

Notifies the accounting server of the results of Web authentication.

Syntax

To set information:

aaa accounting web-authentication default start-stop group radius

To delete information:

no aaa accounting web-authentication default

Input mode

(config)

Parameters

None

Default behavior

Notification to the accounting server is only performed after this is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa authentication web-authentication default group radius

Sets whether to use the RADIUS server for Web authentication.

Syntax

To set information:

aaa authentication web-authentication default group radius

To delete information:

no aaa authentication web-authentication default

Input mode

(config)

Parameters

None

Default behavior

User authentication is performed by using the internal Web authentication database instead of using the RADIUS server.

Impact on communication

Authentications for all users will be canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Before entering this command, set RADIUS server authentication settings.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa accounting web-authentication default start-stop group radius

web-authentication auto-logout

The `no web-authentication auto-logout` command configures the Switch to detect terminals that have been authenticated by Web authentication but have not been used for a certain period of time, and cancels authentication for these terminals.

Syntax

To set information:

no web-authentication auto-logout

To delete information:

web-authentication auto-logout

Input mode

`(config)`

Parameters

None

Default behavior

If the Switch detects MAC addresses that have been authenticated by Web authentication but have not been used for a certain period of time on the MAC address table, authentication for these MAC addresses is canceled.

Impact on communication

When this command is executed, even if the Switch detects MAC addresses that have been authenticated by Web authentication but have not been used for a certain period of time, if these MAC addresses remain in the MAC address table, then authentication is not canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

web-authentication system-auth-control

mac-address-table aging-time

web-authentication ip address

Sets the Web authentication IP address.

When the Web authentication IP address has been set by using this command, you can log in from an unauthenticated terminal or log out from an authenticated terminal by using the same IP address on the switch.

Make sure that this command is set in any mode other than legacy mode.

This command also sets the FQDN (fully qualified domain name) corresponding to the Web authentication IP address.

Syntax

To set or change information:

web-authentication ip address <*authentication address*> [fqdn <*fqdn*>]

To delete information:

no web-authentication ip address

Input mode

```
(config)
```

Parameters

<*authentication address*>

Sets the Web authentication IP address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the IPv4 address (dot notation) for <*authentication address*>.

   The following values cannot be set:

   - The IP address set for the loopback interface

   - IP addresses in the subnet set for each interface

fqdn <*fqdn*>

Specifies the FQDN corresponding to the Web authentication IP address.

1. Default value when this parameter is omitted:

   No FQDN is set.

2. Range of values:

   Enclose a character string consisting of 1 to 255 characters in double quotation marks. Use only alphanumeric characters, periods (.), and hyphens (-). Note that you can use only an alphanumeric character as the first character. You do not have to enclose the character string in double quotation marks.

Default behavior

The Web authentication IP address is not set.

Impact on communication

None

When the change is applied

The change is applied after the `restart web-authentication web-server` operation command is used to restart the Web server.

Notes

1. Because the IP address set by using this command is used exclusively for Web authentication access on a switch, the IP address is not sent outside the switch.
2. After this command is set or deleted, a user who is in the process of being authenticated must log in again.
3. After this command is used to set or delete a TCP port number for Web authentication, execute the `restart web-authentication web-server` operation command immediately to restart the Web server.
4. In legacy mode (in an environment without the `web-authentication port` command configured), if you execute the `web-authentication port` command after you specify this command, you must then restart the Web server by using the `restart web-authentication web-server` operation command.

   Also, if you are in legacy mode, in which all `web-authentication port` command settings are deleted, before deleting this command, restart the Web server by using the `restart web-authentication web-server` operation command.

Related commands

web-authentication system-auth-control

web-authentication port

web-authentication jump-url

Specifies the URL of a page to be automatically displayed after displaying the page indicating successful authentication.

Syntax

To set or change information:

web-authentication jump-url <*url*>

To delete information:

no web-authentication jump-url

Input mode

`(config)`

Parameters

<*url*>

Displays the page of the specified URL after the page indicating successful login is displayed.

Enter the URL starting from the first character (for example, http://.....).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string consisting of 1 to 256 characters in double quotation marks. Use only alphanumeric characters and special characters excluding space characters. If an input character string does not include any special characters, you do not have to enclose the character string in double quotation marks. For details, see *Any character string* in *Specifiable values for parameters*.

   Examples

   (config)# web-authentication jump-url "http://www.example.com/"

Default behavior

After successful authentication, only the page indicating successful authentication is displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When replacing the Authentication Success page by using the `set web-authentication html-files` operation command, in the Authentication Success page file (`loginOK.html`), write the tag of the new URL (<*!-- Redirect_URL --*>) that you want the user to be redirected to after successful authentication. This causes the page specified by the URL to appear automatically after successful authentication.

Related commands

web-authentication system-auth-control

web-authentication logging enable

Enables the output of Web authentication operation log information to a syslog server.

Syntax

To set information:

web-authentication logging enable

To delete information:

no web-authentication logging enable

Input mode

(config)

Parameters

None

Default behavior

Operation log information is not output to a syslog server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

web-authentication system-auth-control

logging event-kind

logging email-event-kind

web-authentication logout ping tos-windows

When Web authentication in fixed VLAN mode is used, this command sets the TOS value of special packets to cancel the authentication status of the corresponding MAC address when the special packets (ping) are received from authenticated terminals.

Syntax

To set or change information:

web-authentication logout ping tos-windows <*tos*>

To delete information:

no web-authentication logout ping tos-windows

Input mode

`(config)`

Parameters

<*tos*>

Sets the TOS value of special packets for Web authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 255

Default behavior

The TOS value of special packets is set to 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout ping ttl

web-authentication logout ping ttl

When Web authentication in fixed VLAN mode is used, this command sets the TTL value of special packets to cancel the authentication status of the corresponding MAC address when the special packets (ping) are received from authenticated terminals.

Syntax

To set or change information:

web-authentication logout ping ttl <*ttl*>

To delete information:

no web-authentication logout ping ttl

Input mode

(config)

Parameters

<*ttl*>

Sets the TTL value of special packets for Web authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

The TTL value of special packets is set to 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout ping tos-windows

web-authentication logout polling count

When Web authentication in fixed VLAN mode is used, this command sets the number of times a Switch retransmits the monitoring packet that is sent periodically to check the connection status of authentication terminals when there is no response to the monitoring packet.

Syntax

To set or change information:

web-authentication logout polling count <*count*>

To delete information:

no web-authentication logout polling count

Input mode

(config)

Parameters

<*count*>

Sets the number of times a Switch retransmits a monitoring packet when there is no response to the monitoring packet.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10 (times)

Default behavior

Monitoring packets are retransmitted a maximum of three times.

Impact on communication

None

When the change is applied

The setting takes effect when the first sending interval has passed since the value was changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If link-down status for a monitored port is detected before periodic monitoring using the logout monitoring functionality detects no response, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time expires, the Switch stops monitoring the applicable VLAN.
4. If the number of retransmissions when a no-response state is detected is set to maximum, the number of monitoring packets increases in proportion to the number of authenticated users, and might be a heavy load on the switch.

   Set the polling interval by using the following formula as a guide

   Polling condition:

   (1) *polling interval* > (2) *polling retry-interval* x (3) *polling count*

   Set each value so that retransmission when a no-response state is detected does not

exceed the polling interval, so that the retransmission can complete during one polling interval.

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

- If the number of authenticated terminals exceeds 2000, do not specify a value smaller than 300 seconds for the monitoring packet sending interval.
- If the number of authenticated terminals is less than 2000 and the monitoring packet sending interval is configured to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling enable

Set this command to periodically check whether authenticated terminals are connected, and forcibly log out inactive or disconnected terminals when Web authentication is used in fixed VLAN mode.

Periodic monitoring is not performed if the setting of forcible logout based on periodic check is disabled by using the `no web-authentication logout polling enable` command.

Syntax

To set information:

no web-authentication logout polling enable

To delete information:

web-authentication logout polling enable

Input mode

`(config)`

Parameters

None

Default behavior

Authenticated terminals are monitored at the following intervals:

Polling interval

The interval set by using the `web-authentication logout polling interval` command. 300 seconds is set by default.

Retransmission interval

The interval set by using the `web-authentication logout polling retry-interval` command. 1 second is set by default.

Number of retransmissions

The number of retransmissions set by using the `web-authentication logout polling count` command. Three retransmissions is set by default.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If the link for the applicable port goes down, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time (set by using the `web-authentication max-timer` command) expires, the Switch stops monitoring the applicable terminal and logs it out.
4. If the sending interval time (set by using the `web-authentication logout polling interval` command) is set to the minimum value, the number of monitoring packets increases in proportion to the number of authenticated users, and might be a heavy load on the switch.

If the number of retransmissions when a no-response state is detected is set to the maximum (it is set by using the `web-authentication logout polling count` command) and the resending interval time is set to the minimum (it is set by using the `web-authentication logout polling retry-interval` command), this also might be a heavy load on the switch.

Set the polling interval by using the following formula as a guide:

Polling condition:

(1) *polling interval* > (2) *polling retry-interval* x (3) *polling count*

Set each value so that retransmission when a no-response state is detected does not exceed the polling interval, so that the retransmission can complete during one polling interval.

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

- If the number of authenticated terminals exceeds 2000, do not specify a value smaller than 300 seconds for the monitoring packet sending interval.
- If the number of authenticated terminals is less than 2000 and the monitoring packet sending interval is configured to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling count

web-authentication logout polling interval

Sets the sending interval of monitoring packets that periodically check whether authenticated terminals are connected when Web authentication in fixed VLAN mode is used.

Syntax

To set or change information:

web-authentication logout polling interval <*seconds*>

To delete information:

no web-authentication logout polling interval

Input mode

(config)

Parameters

<*seconds*>

Sets the sending interval of monitoring packets.

The setting is configured for each switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   60 to 86400 (seconds)

Default behavior

Monitoring packets are sent every 300 seconds to an authenticated terminal only if the logout monitoring command (the `web-authentication logout polling enable` command) has been set.

Impact on communication

None

When the change is applied

The setting takes effect when the first sending interval has passed since the value was changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If link-down status for a monitored port is detected before periodic monitoring using the logout monitoring functionality detects no response, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time expires, the Switch stops monitoring the applicable terminals.
4. If the sending interval is set to the minimum, the number of monitoring packets increases proportionately with the number of authenticated users, which might be a heavy load on the switch.

   Set the polling interval by using the following formula as a guide:

   Polling condition:

   (1) *polling interval* > (2) *polling retry-interval* x (3) *polling count*

Set each value so that retransmission when a no-response state is detected does not exceed the polling interval, so that the retransmission can complete during one polling interval.

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

- If the number of authenticated terminals exceeds 2000, do not specify a value smaller than 300 seconds for the monitoring packet sending interval.
- If the number of authenticated terminals is less than 2000 and the monitoring packet sending interval is configured to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling enable

web-authentication logout polling retry-interval

web-authentication logout polling count

web-authentication logout polling retry-interval

When Web authentication in fixed VLAN mode is used, this command sets the sending interval for retransmitting the monitoring packet when there is no response to a monitoring packet that periodically checks the connection status of authenticated terminals.

Syntax

To set or change information:

web-authentication logout polling retry-interval <*seconds*>

To delete information:

no web-authentication logout polling retry-interval

Input mode

```
(config)
```

Parameters

<*seconds*>

Sets the retransmission interval of monitoring packets.

The setting is configured for each switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10 (seconds)

Default behavior

The retransmission interval of monitoring packets is 1 second.

Impact on communication

None

When the change is applied

The setting takes effect when the first sending interval has passed since the value was changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If link-down status for a monitored port is detected before periodic monitoring using the logout monitoring functionality detects no response, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time expires, the Switch stops monitoring the applicable terminals.
4. If the retransmission interval is set to the minimum, the number of monitoring packets increases in proportion to the number of authenticated users, which might be a heavy load on the switch.

   Set the polling interval by using the following formula as a guide:

   Polling condition:

   (1) *polling interval* > (2) *polling retry-interval* x (3) *polling count*

Set each value so that retransmission when a no-response state is detected does not exceed the polling interval, so that the retransmission can complete during one polling interval.

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

- If the number of authenticated terminals exceeds 2000, do not specify a value smaller than 300 seconds for the monitoring packet sending interval.
- If the number of authenticated terminals is less than 2000 and the monitoring packet sending interval is configured to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication static-vlan max-user

web-authentication port

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication logout polling count

web-authentication max-timer

Specifies the maximum connection time for Web-authenticated users.

Syntax

To set or change information:

web-authentication max-timer <*minutes*>

To delete information:

no web-authentication max-timer

Input mode

`(config)`

Parameters

<*minutes*>

Sets the maximum time (in minutes) a user is allowed for connection for authentication in the Web authentication system. After a user logs in, if the time set by using this command elapses, the authentication is automatically canceled. Cancellation of the authentication is performed within a minute after the set time elapses.

If `infinity` is specified, the maximum connection time is set to infinity, and authentication is not canceled based on the maximum connection time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 1440, or `infinity`

Default behavior

60 minutes is set as the maximum connection time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the value for the maximum connection time is either decreased or increased, the previous setting is applied to users that are currently authenticated, and the new configuration setting takes effect only from the next login of a new user.
2. The connection time for Web authentication is calculated using the clock in the switch. Accordingly, if the date and time are changed by using the `set clock` operation command, the connection time is affected.

   Example:

   If you advance the clock by three hours, sessions will appear to have been in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, sessions will be extended by three hours.

Related commands

web-authentication system-auth-control

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication max-user

Sets the maximum number of Web-authenticated users allowed in dynamic VLAN mode or legacy mode.

Syntax

To set or change information:

web-authentication max-user <*count*>

To delete information:

no web-authentication max-user

Input mode

(config)

Parameters

<*count*>

Sets the maximum number of users that can be authenticated by Web authentication. More users than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4096

Default behavior

The maximum users that can be authenticated is 4096.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to users that have already been authenticated, and takes effect only from the next login.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication port

Sets Web authentication for the specified port.

If this command is set for an access port or a trunk port, fixed VLAN mode is set. If this command is set to a MAC VLAN, dynamic VLAN mode is set.

Syntax

To set information:

web-authentication port

To delete information:

no web-authentication port

Input mode

`(config-if)`

Parameters

None

Default behavior

If this command has not been set, the Switch operates as usual.

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 when the `web-authentication vlan` command has been set.
2. The applicable port cannot be set to dynamic VLAN mode if this command has been used to set another authenticating port to fixed VLAN mode. Likewise, the applicable port cannot be set to fixed VLAN mode if another authenticating port has been set to dynamic VLAN mode.
3. In legacy mode, if the `web-authentication ip address` command is set before this command is set, first set this command, and then use the `restart web-authentication web-server` operation command to restart the Web server.

   After this command is deleted, if the `web-authentication ip address` command is set in legacy mode (which does not support setting of this command), use the `restart web-authentication web-server` operation command to restart the Web server.

Related commands

web-authentication ip address

web-authentication system-auth-control

web-authentication redirect-mode

Sets a protocol to display the Login page when URL redirect functionality is enabled in Web authentication.

Syntax

To set or change information:

web-authentication redirect-mode {http | https}

To delete information:

no web-authentication redirect-mode

Input mode

`(config)`

Parameters

{http | https}

http

The Login page for http is displayed when the URL redirect functionality is enabled.

https

The Login page for https is displayed when the URL redirect functionality is enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `http` or `https`

Default behavior

The Login page for https is displayed when this command is omitted.

Impact on communication

None

When the change is applied

The change is applied after the `restart web-authentication web-server` operation command is used to restart the Web server.

Notes

1. This command setting is enabled only when the VLAN for which URL redirection is used is set by using the `web-authentication redirect-vlan` command.

Related commands

web-authentication port

web-authentication redirect-vlan

web-authentication system-auth-control

web-authentication redirect-vlan

Specifies the native VLAN for a MAC port for which dynamic VLAN mode is to be set. This setting is required before the URL redirect functionality is used.

Syntax

To set or change information:

web-authentication redirect-vlan <*vlan id list*>

To delete information:

no web-authentication redirect-vlan

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies pre-authorized VLANs to be used in dynamic VLAN mode. Changing the parameter replaces the existing VLAN with the VLAN that has been set. You cannot specify a MAC VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied after the `restart web-authentication web-server` operation command is used to restart the Web server.

Notes

1. For the pre-authenticated VLANs specified in this command, communication on http and https ports is restricted.
2. Set the pre-authentication VLAN specified in this command for the native VLAN for the MAC port for which dynamic VLAN mode is set.

Related commands

switchport mac native vlan

web-authentication static-vlan max-user

Sets the maximum number of Web-authenticated users allowed in fixed VLAN mode.

Syntax

To set or change information:

web-authentication static-vlan max-user <*count*>

To delete information:

no web-authentication static-vlan max-user

Input mode

(config)

Parameters

<*count*>

Sets the maximum number of Web-authenticated users allowed in fixed VLAN mode.

More users than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4096

Default behavior

The maximum users that can be authenticated: 4096 users

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to users that have already been authenticated, and takes effect only from the next login.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling count

web-authentication system-auth-control

Starts the Web authentication daemon, and enables Web authentication.

Note that if the `no web-authentication system-auth-control` command is executed, the Web authentication daemon stops.

Syntax

To set information:

web-authentication system-auth-control

To delete information:

no web-authentication system-auth-control

Input mode

`(config)`

Parameters

None

Default behavior

Web authentication is not performed.

Impact on communication

If the `no web-authentication system-auth-control` command is executed, authentication of the authenticated users is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `no web-authentication system-auth-control` command is executed, user information registered in the internal Web authentication database is saved in its current state.
2. This command cannot be set if an authentication VLAN has been set.
3. After you stop Web authentication by using the `no web-authentication system-auth-control` command, wait at least 10 seconds before using the `web-authentication system-auth-control` command to restart Web authentication.

Related commands

web-authentication max-timer

web-authentication max-user

web-authentication vlan

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication vlan

Specifies the ID of the VLAN that is allowed to be switched in legacy mode of Web authentication.

Unless a VLAN ID is not set by using this command, no VLANs can be switched after authentication.

Syntax

To set or change information:

web-authentication vlan <*vlan id list*>

To delete information:

no web-authentication vlan <*vlan id list*>

Input mode

`(config)`

Parameters

<*vlan id list*>

Specifies the VLAN list for the MAC VLAN that is to be switched after user authentication in Web authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*. Note that it cannot be specified for the default VLAN (VLAN ID = 1).

Default behavior

No VLANs are switched after authentication.

Impact on communication

If VLANs are deleted by using this command, authentication of users registered in the VLAN you have deleted is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All VLAN IDs you have specified must be set for a MAC VLAN.
2. This command cannot be set when the `web-authentication port` command has been set.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication max-user

web-authentication auto-logout

aaa authentication web-authentication default group radius

aaa accounting web-authentication default start-stop group radius

web-authentication web-port

Adds a TCP port number for Web authentication to any port number.

Usually, any port numbers can be added to the standard port numbers assigned for http (80) and https (443). This command can be used in any of the following modes: legacy mode, dynamic VLAN mode, or fixed VLAN mode.

Note that, if AX-Config-Master is connected to the authenticating port in fixed VLAN mode or dynamic VLAN mode, you must specify the port number used by OAN (https: 832 and 9698).

Syntax

To set or change information:

web-authentication web-port {http | https} <*port*> [<*port*>]

To delete information:

no web-authentication web-port {http | https}

Input mode

`(config)`

Parameters

{http | https}

http

Adds a TCP port number for http.

https

Adds a TCP port number for https.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `http` or `https`

<*port*>

Sets the port number to be used for communication in http or https protocol to be added.

Note that if OAN is also used, port numbers 832 and 9698 are used by OAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   832 or 1024 to 65535

Default behavior

The following initial port numbers are used for communication:

- http: 80
- https: 443

Impact on communication

None

When the change is applied

The change is applied after the `restart web-authentication web-server` operation command is used to restart the Web server.

Notes

1. After this command is set or deleted, a user who is in the process of being authenticated must log in again.
2. If OAN is also used, the port numbers 832 and 9698, which are used by OAN, cannot be used for login and logout operations for Web authentication.
3. After this command is used to set or delete a TCP port number for Web authentication, execute the `restart web-authentication web-server` operation command immediately to restart the Web server.

Related commands

web-authentication system-auth-control

web-authentication vlan

web-authentication port

restart web-authentication

Chapter

11. MAC-based authentication

Correspondence between configuration commands and operation modes

The following table describes MAC-based authentication operation modes in which MAC-based authentication configuration commands can be set.

Table 11-1: Configuration commands and MAC-based authentication operation modes

Command name	MAC-based authentication operation modes	
	Fixed VLAN mode	Dynamic VLAN mode
aaa accounting mac-authentication default start-stop group radius	Y	Y
aaa authentication mac-authentication default group radius	Y	Y
authentication ip access-group	Y	Y
mac-authentication auth-interval-timer	Y	Y
mac-authentication auto-logout	Y	Y
mac-authentication dynamic-vlan max-user	--	Y
mac-authentication logging enable	Y	Y
mac-authentication max-timer	Y	Y
mac-authentication password	Y	Y
mac-authentication port	Y	Y
mac-authentication radius-server host	Y	Y
mac-authentication static-vlan max-user	Y	--
mac-authentication system-auth-control	Y	Y
mac-authentication vlan-check	Y	--

Legend:

Y: The command can be set, and the setting is applied.

--: The command can be set, but the setting is not applied.

aaa accounting mac-authentication default start-stop group radius

Notifies the accounting server of the results of MAC-based authentication.

Syntax

To set information:

aaa accounting mac-authentication default start-stop group radius

To delete information:

no aaa accounting mac-authentication default

Input mode

(config)

Parameters

None

Default behavior

Notification to the accounting server is only performed after this is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

mac-authentication system-auth-control

mac-authentication port

mac-authentication radius-server host

aaa authentication mac-authentication default group radius

radius-server host

aaa authentication mac-authentication default group radius

Sets whether to use the RADIUS server for MAC-based authentication.

Syntax

To set information:

aaa authentication mac-authentication default group radius

To delete information:

no aaa authentication mac-authentication default

Input mode

(config)

Parameters

None

Default behavior

Authentication is performed by using the internal MAC-based authentication database instead of using the RADIUS server.

Impact on communication

All authentications are canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Before setting this command, set RADIUS server authentication settings.

Related commands

mac-authentication system-auth-control

mac-authentication port

mac-authentication radius-server host

radius-server host

mac-authentication auth-interval-timer

Sets the time interval until the next authentication is performed for a MAC address that has failed MAC-based authentication.

Syntax

To set or change information:

mac-authentication auth-interval-timer <*minutes*>

To delete information:

no mac-authentication auth-interval-timer

Input mode

(config)

Parameters

<*minutes*>

Sets the time interval (in minutes) until the next authentication is performed after authentication has failed once.

The next authentication starts within a minute after the set time has elapsed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1440

Default behavior

The time interval until the next authentication is performed is set to the default value (five minutes).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the time is set or changed, the old setting is applied to users that have already been authenticated, and the new configuration setting takes effect only from the next authentication.
2. The connection time for MAC-based authentication is calculated using the clock in the switch. Accordingly, if the date and time is changed by using the `set clock` operation command, the set time is affected.

   Example:

   If you advance the clock by three hours, sessions will appear to be in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, sessions will be extended by three hours from the set time.

Related commands

mac-authentication system-auth-control

mac-authentication port

mac-authentication auto-logout

The `no mac-authentication auto-logout` command configures a Switch so that the Switch detects MAC addresses being authenticated by MAC-based authentication but have not been used for a certain period of time, and cancels the authentication for these MAC addresses.

If automatic cancellation is disabled, authentication is not automatically canceled even when the Switch detects, on the MAC address table, that a MAC address being authenticated by MAC-based authentication is not being used.

Syntax

To set information:

no mac-authentication auto-logout

To delete information:

mac-authentication auto-logout

Input mode

`(config)`

Parameters

None

Default behavior

If the Switch detects on the MAC address table, that a MAC address being authenticated by MAC-based authentication has not been used for a certain period of time, the authentication is canceled.

Impact on communication

If this command is executed, even when the Switch detects the MAC addresses that are being authenticated by MAC-based authentication but have not been used for a certain period of time on the MAC address table, authentication for these MAC addresses is not canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If canceling authentication when no access is detected is set for a MAC address being authenticated by MAC-based authentication (by default, or when this command is deleted), authentication for the MAC address is canceled after the aging time for the MAC address table expires.

Related commands

max-authentication system-auth-control

mac-address-table aging-time

mac-authentication dynamic-vlan max-user

Sets the maximum number of MAC addresses that can be authenticated in dynamic VLAN mode of MAC-based authentication.

Syntax

To set or change information:

mac-authentication dynamic-vlan max-user <*count*>

To delete information:

no mac-authentication dynamic-vlan max-user

Input mode

(config)

Parameters

<*count*>

Sets the maximum number of MAC addresses that can be authenticated in dynamic VLAN mode of MAC-based authentication. More MAC addresses than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4096

Default behavior

The maximum number of MAC addresses that can be authenticated:

4096

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to MAC addresses that have already been authenticated, and takes effect only from the next login.

Related commands

mac-authentication system-auth-control

mac-authentication logging enable

Enables the output of operation log information for MAC-based authentication to a syslog server.

Syntax

To set information:

mac-authentication logging enable

To delete information:

no mac-authentication logging enable

Input mode

(config)

Parameters

None

Default behavior

Operation log information is not output to a syslog server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

mac-authentication system-auth-control

logging event-kind

logging email-event-kind

mac-authentication max-timer

Sets the maximum connection time used for MAC-based authentication.

Syntax

To set or change information:

mac-authentication max-timer {<*minutes*> | infinity}

To delete information:

no mac-authentication max-timer

Input mode

`(config)`

Parameters

{<*minutes*> | infinity}

Sets the maximum connection time (in minutes) used for MAC-based authentication. After a successful authentication, if the period of time set by using this command elapses, the authentication is canceled automatically. Cancellation of the authentication is performed within a minute after the set time elapses.

If `infinity` is specified, the maximum connection time is set to infinity, and authentication is not canceled based on the maximum connection time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 1440, or `infinity`

Default behavior

Authentication is not cancelled based on the maximum connection time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the value for the maximum connection time is either decreased or increased, the previous setting is applied to a MAC address that is currently authenticated, and the configuration setting takes effect only from the next login.
2. The connection time for MAC-based authentication is calculated using the clock in the switch. Accordingly, if the date and time are changed by using the `set clock` operation command, the connection time is affected.

   Example:

   If you advance the clock by three hours, sessions will appear to have been in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, sessions will be extended by three hours.

Related commands

mac-authentication system-auth-control

mac-authentication port

mac-authentication password

Sets the password used by the terminal user when the user issues a MAC-based authentication request to the RADIUS server.

Syntax

To set or change information:

mac-authentication password <*password*>

To delete information:

no mac-authentication password

Input mode

(config)

Parameters

<*password*>

Sets the user information password for when a user issues a MAC-based authentication request to the RADIUS server

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string consisting of 1 to 32 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

If this command is not set, the MAC address of the terminal to be authenticated is used as the user information password.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication default group radius

mac-authentication port

Specifies a port for which MAC-based authentication is to be performed.

MAC-based authentication does not work on any ports for which this command is not set.

If this command is set for an access port or a trunk port, fixed VLAN mode is set. If this command is set to a MAC VLAN, dynamic VLAN mode is set.

Syntax

To set information:

mac-authentication port

To delete information:

no mac-authentication port

Input mode

(config-if)

Parameters

None

Default behavior

MAC-based authentication is not performed for the port.

Impact on communication

If a port subject to authentication is deleted by using this command, authentication is canceled on all applicable ports.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

mac-authentication system-auth-control

mac-authentication radius-server host

Configures the RADIUS server used for MAC-based authentication.

Syntax

To set information:

mac-authentication radius-server host {<*ipv4 address*> | <*ipv6 address*> [interface <*interface type*> <*interface number*>] | <*host name*>} [auth-port <*port*>][acct-port <*port*>][timeout <*seconds*>][retransmit <*retries*>][key <*string*>]

To delete information:

no mac-authentication radius-server host {<*ipv4 address*> | <*ipv6 address*> [interface <*interface type*> <*interface number*>] | <*host name*>}

Input mode

`(config)`

Parameters

{<*ipv4 address*> | <*ipv6 address*> [interface <*interface type*> <*interface number*>] | <*host name*>}

<*ipv4 address*>

Specifies the IPv4 address of the RADIUS server in dot notation.

<*ipv6 address*> [interface <*interface type*> <*interface number*>]

Specifies the IPv6 address of the RADIUS server in colon notation.

Specify the `interface` parameter only when a link-local address is specified.

For <*interface type*> <*interface number*>, the following values can be specified:

- vlan <*vlan id*>

  For <*vlan id*>, specify the VLAN ID set by the `interface vlan` command.

- mgmt `0`

<*host name*>

Specifies the host name of the RADIUS server with 64 or fewer characters.

For details about the characters that can be specified for the host name, see *Specifiable values for parameters*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address, an IPv6 address, or a host name can be specified.

   If an IPv6 link-local address is specified, also specify the interface.

auth-port <*port*>

Specifies the RADIUS server port number.

1. Default value when this parameter is omitted:

   Port number 1812 is used.

2. Range of values:

1 to 65535

acct-port <*port*>

Specifies the port number for RADIUS server accounting.

1. Default value when this parameter is omitted:

   Port number 1813 is used.

2. Range of values:

   1 to 65535

timeout <*seconds*>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   5

2. Range of values:

   1 to 30 (seconds)

retransmit <*retries*>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   3

2. Range of values:

   0 to 15 (times)

key <*string*>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   The RADIUS key set by using `radius-server key` is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Enclose a character string consisting of 1 to 64 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 RADIUS server settings registered by using the `radius-server host` command are used.

If the `radius-server host` command is not registered, authentication cannot be performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is executed, the setting information of the RADIUS server referenced by MAC-based authentication has precedence over the information set by using the `radius-server host` command.
2. A maximum of four RADIUS servers per switch can be set by this command.
3. If multiple RADIUS servers are set by using this command, the RADIUS server listed at the top of the display resulting from this configuration command is used for the first authentication.

Related commands

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication default group radius

aaa accounting mac-authentication default start-stop group radius

radius-server host

mac-authentication static-vlan max-user

Sets the maximum number of MAC addresses that can be authenticated in fixed VLAN mode of MAC-based authentication.

Syntax

To set or change information:

mac-authentication static-vlan max-user <*count*>

To delete information:

no mac-authentication static-vlan max-user

Input mode

(config)

Parameters

<*count*>

Sets the maximum number of MAC addresses that can be authenticated in fixed VLAN mode of MAC-based authentication. More MAC addresses than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4096

Default behavior

The maximum number of MAC addresses that can be authenticated: 4096

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to MAC addresses that have already been authenticated, and takes effect only from the next login.

Related commands

mac-authentication system-auth-control

mac-authentication port

mac-authentication system-auth-control

Starts the MAC-based authentication daemon, and enables MAC-based authentication.

Note that if the `no mac-authentication system-auth-control` command is executed, the MAC-based authentication daemon stops.

Syntax

To set information:

mac-authentication system-auth-control

To delete information:

no mac-authentication system-auth-control

Input mode

`(config)`

Parameters

None

Default behavior

MAC-based authentication is not performed.

Impact on communication

If the `no mac-authentication system-auth-control` command is executed, all authentications are canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set if an authentication VLAN has been set.

Related commands

mac-authentication port

mac-authentication vlan-check

When a MAC address is checked in fixed VLAN mode of MAC-based authentication, the VLAN ID is also checked.

Syntax

To set or change information:

mac-authentication vlan-check [key <*string*>]

To delete information:

no mac-authentication vlan-check

Input mode

`(config)`

Parameters

key <*string*>

Sets a character string to be added to the account that is used for a request to the RADIUS server in fixed VLAN mode of MAC-based authentication. For an account used by the Switch when submitting requests to the RADIUS server for MAC-based authentication, a combination of the MAC address string, the character string set by this command, and the VLAN ID string is used.

1. Default value when this parameter is omitted:

   `%VLAN` is set.

2. Range of values:

   Enclose a character string consisting of 1 to 64 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*.

   Example: If `@vlan` is set, the user information (for MAC address `0012.e201.23ab`, and vlan id `10`) sent to the RADIUS server is `0012e20123ab@vlan10`.

Default behavior

A VLAN ID is not checked for authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication default group radius

Chapter

12. Authentication VLANs [OP-VAA]

fense alive-timer [OP-VAA]
fense retry-count [OP-VAA]
fense retry-timer [OP-VAA]
fense server [OP-VAA]
fense vaa-name [OP-VAA]
fense vaa-sync [OP-VAA]
fense vlan [OP-VAA]

fense alive-timer [OP-VAA]

If a KeepAlive packet does not arrive from the VLANaccessController within the time period (in seconds) specified by this command, the switch will attempt to re-establish the connection to the authentication server.

Syntax

To set or change information:

fense <*vaa id*> alive-timer <*seconds*>

To delete information:

no fense <*vaa id*> alive-timer

Input mode

`(config)`

Parameters

<*vaa id*>

Specifies the number the Switch uses to identify the connection to the VLANaccessController in the authentication VLAN system.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

<*seconds*>

Specifies the time interval (in seconds) between monitoring Keep Alive packets sent from VLANaccessController.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   20 to 7200

Default behavior

<*seconds*> is set to 20.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `dot1x system-auth-control` command is set for IEEE 802.1X, this command cannot be set.

Related commands

fense vaa-name

fense server

fense vlan

fense retry-count [OP-VAA]

If a VLANaccessAgent fails to connect to the VLANaccessController, the VLANaccessAgent retries connection at the interval specified by the `fense retry-timer` command. The retries continue unless the `no fense server` command is executed. However, if the total number of failed retries performed by all VLANaccessAgents running on the Switch exceeds the allowed number of failed retries set by this command, dynamic MAC addresses for all authentication VLANs in the Switch are deleted.

Syntax

To set or change information:

fense <*vaa id*> retry-count { <*count*> | infinity }

To delete information:

no fense <*vaa id*> retry-count

Input mode

`(config)`

Parameters

<*vaa id*>

Specifies the number the Switch uses to identify the connection to the VLANaccessController in the authentication VLAN system.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

{ <*count*> | infinity }

If `infinity` is specified for one or more VLANaccessAgents, dynamic MAC addresses for authentication VLANs are not all deleted, and connection retries will be performed infinitely.

If 0 is specified for the argument of this command, the Switch tries to delete dynamic MAC addresses for authentication VLANs every time a retry fails.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `infinity`, or 0 to 32767

Default behavior

<*count*> is set to 25920.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `dot1x system-auth-control` command is set for IEEE 802.1X, this command cannot

be set.

Related commands

fense vaa-name

fense server

fense vlan

fense retry-timer [OP-VAA]

If communication with the VLANaccessController fails, the Switch retries connection at the interval (in seconds) set by this command.

Syntax

To set or change information:

fense <*vaa id*> retry-timer <*seconds*>

To delete information:

no fense <*vaa id*> retry-timer

Input mode

`(config)`

Parameters

<*vaa id*>

Specifies the number the Switch uses to identify the connection to the VLANaccessController in the authentication VLAN system.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

<*seconds*>

Specifies the retry interval in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

<*seconds*> is set to 10.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `dot1x system-auth-control` command is set for IEEE 802.1X, this command cannot be set.

Related commands

fense vaa-name

fense server

fense vlan

fense server [OP-VAA]

Specifies the IP address and TCP port number of the authentication server (VLANaccessController).

Syntax

To set or change information:

fense <*vaa id*> server <*server address*> [<*port*>]

To delete information:

no fense <*vaa id*> server

Input mode

(config)

Parameters

<*vaa id*>

Specifies the number the Switch uses to identify the connection to the VLANaccessController in the authentication VLAN system.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

<*server address*>

Specifies the IPv4 address of the VLANaccessController in dot notation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies the IPv4 address of the VLANaccessController in dot notation.

<*port*>

Specifies the TCP port number of the VLANaccessController.

1. Default value when this parameter is omitted:

   52153

2. Range of values:

   1024 to 65535

Default behavior

None

Impact on communication

If the authentication server is changed by using this command, communication with the old server is cut off, and communication with the new server starts. Communications for authenticated clients are not affected.

When the change is applied

The change is applied immediately after setting values are changed.

If any of the following conditions are satisfied, the VLANaccessAgent is started, and connection to the authentication server is started:

- The device name has been set by the `fense vaa-name` command.
- The authentication server has been configured by the `fense server` command.
- One or more entries have been set by the `fense vlan` command.

Notes

1. If the `dot1x system-auth-control` command is set for IEEE 802.1X, this command cannot be set.
2. If you have modified the network configuration of an authentication VLAN system by using the `fense vlan` command, be sure to restart the functions of the authentication server, and then restart the authentication VLANs on the Switch.
3. If the same <*server address*> is specified for multiple <*vaa id*> by using this command, connection to the authentication server might become unstable. In such a case, review the network configuration to reset the authentication VLAN configuration, and then restart the authentication VLANs on the Switch.
4. If you set a `fense vlan` command with a <*vaa id*> that is the same as already registered by the `fense server` command, the `no fense server` command cannot delete the setting. First execute the `no fense vlan` command, and then execute the `no fense server` command.

Related commands

fense vaa-name

fense vlan

fense vaa-name [OP-VAA]

Sets the name of the VLANaccessAgent that sends packets to the VLANaccessController. Only one name can be set per switch. If multiple switches on which the VLANaccessAgent runs are connected under the authentication server, set different names for the switches.

Syntax

To set or change information:

fense vaa-name <*name*>

To delete information:

no fense vaa-name

Input mode

`(config)`

Parameters

<*name*>

Specifies the name of the VLANaccessAgent that sends packets to the VLANaccessController. Only one name can be set per switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 64 characters. Only alphanumeric characters, forward slashes (/), hyphens (-), underscores (_), and periods (.) can be used. The following character strings cannot be specified:

   . (The first character is a period.)

   ID

   DPCI

   VLAN

   MAC

   -ERR

Default behavior

None

Impact on communication

If vaa-name is changed or deleted by this command, communication between the VLANaccessAgent and the authentication server is temporarily disconnected and then reconnected, which does not affect communication for authenticated clients.

When the change is applied

The change is applied immediately after setting values are changed.

If any of the following conditions are satisfied, the VLANaccessAgent is started, and connection to the authentication server is started:

- The device name has been set by the `fense vaa-name` command.
- The authentication server has been configured by the `fense server` command.

- One or more entries have been set by the `fense vlan` command.

Notes

1. If the `dot1x system-auth-control` command is set for IEEE 802.1X, this command cannot be set.
2. When you have modified the network configuration of an authentication VLAN system by using this command, be sure to restart the functions of the authentication server, and then restart the authentication VLANs on the Switch.

Related commands

fense server

fense vlan

fense vaa-sync [OP-VAA]

The Switch operates in normal mode for a MAC address registration request for MAC VLANs from the authentication server. If `no fense vaa-sync` is set, the Switch operates in selective registration mode.

Syntax

To set information:

no fense vaa-sync

To delete information:

fense vaa-sync

Input mode

`(config)`

Parameters

None

Default behavior

The Switch operates in normal mode.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

fense vaa-name

fense vlan [OP-VAA]

Specifies the VLAN ID and subnet of the authorized VLAN.

Syntax

To set or change information:

fense <*vaa id*> vlan <*vlan id*> <*subnet address*> <*subnet mask*>

To delete information:

no fense <*vaa id*> vlan <*vlan id*> <*subnet address*> <*subnet mask*>

Input mode

`(config)`

Parameters

<*vaa id*>

Specifies the number the Switch uses to identify the connection to VLANaccessController in the authentication VLAN system.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

<*vlan id*>

Specifies the VLAN ID of the authenticated VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the VLAN ID specified for the MAC VLAN.

<*subnet address*>

Specify the subnet address of the authenticated VLAN in dot notation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the subnet address of the authenticated VLAN in dot notation.

<*subnet mask*>

Specifies the subnet mask of the authorized VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   128.0.0.0 to 255.255.255.255

Default behavior

None

Impact on communication

If an authenticated VLAN is changed or deleted by this command, communication between the VLANaccessAgent and the authentication server is temporarily disconnected and then reconnected, which does not affect communication for authenticated clients.

When the change is applied

The change is applied immediately after setting values are changed.

If any of the following conditions are satisfied, the VLANaccessAgent is started, and connection to the authentication server is started:

- The device name has been set by the `fense vaa-name` command.
- The authentication server has been configured by the `fense server` command.
- One or more entries have been set by the `fense vlan` command.

Notes

1. A MAC VLAN must be configured on the VLAN corresponding to the VLAN ID.
2. For <*vaa id*>, you cannot specify a subnet different from the subnet that has already been set for the corresponding VLAN ID.
3. By using <*vaa id*>, you can set no more than 4094 `fense vlan` command settings on a switch. Note that, if the same VLAN ID is assigned to multiple <*vaa id*>, each is counted as one setting.
4. If the `dot1x system-auth-control` command is set for IEEE 802.1X, this command cannot be set.
5. When you have modified the network configuration of an authentication VLAN system by using this command, be sure to restart the functions of the authentication server, and then restart the authentication VLANs on the Switch.

Related commands

fense vaa-name

fense server

Chapter 13. DHCP Snooping

ip arp inspection limit rate
ip arp inspection trust
ip arp inspection validate
ip arp inspection vlan
ip dhcp snooping
ip dhcp snooping database url
ip dhcp snooping database write-delay
ip dhcp snooping information option allow-untrusted
ip dhcp snooping limit rate
ip dhcp snooping logging enable
ip dhcp snooping loglevel
ip dhcp snooping trust
ip dhcp snooping verify mac-address
ip dhcp snooping vlan
ip source binding
ip verify source

ip arp inspection limit rate

Sets the maximum ARP packet reception rate (the number of ARP packets that can be received per second) per Switch when DHCP snooping is enabled on the Switch. ARP packets in excess of this reception rate are discarded. The actual maximum reception rate is the sum of that set by this command and that set by the `ip dhcp snooping limit rate` command. The number of packets that can be received is the total number of DHCP packets and ARP packets.

Syntax

To set or change information:

ip arp inspection limit rate <*packet/s*>

To delete information:

no ip arp inspection limit rate

Input mode

`(config)`

Parameters

<*packet/s*>

Sets the number of ARP packets that can be received per second.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 125 (packets/s)

Default behavior

The reception rate is not restricted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Values specified by using this command set the upper limit for the number of received packets, but do not guarantee operation with the specified value.

Related commands

ip dhcp snooping

ip arp inspection trust

Sets the applicable interface as a trusted port where no dynamic ARP inspection is performed when DHCP snooping is enabled on a Switch.

Syntax

To set information:

ip arp inspection trust

To delete information:

no ip arp inspection trust

Input mode

(config-if)

Parameters

None

Default behavior

Dynamic ARP inspection is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. On an interface on which this command is set, if the interface is accommodated in the VLAN where dynamic ARP inspection is enabled, the inspection of ARP packets is not performed.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip arp inspection validate

Sets inspection items to be added to improve the accuracy of a dynamic ARP inspection when dynamic ARP inspections are enabled on a Switch.

Syntax

To set or change information:

ip arp inspection validate [src-mac] [dst-mac] [ip]

To delete information:

no ip arp inspection validate

Input mode

(config)

Parameters

src-mac

When the src-mac option is specified, the Switch checks whether the source MAC address in the Layer 2 header of the received ARP packet matches the sender MAC address in the ARP header. This inspection is performed on both an ARP request and an ARP reply.

1. Default value when this parameter is omitted:

   When the src-mac option is not specified, the Switch does not check whether the source MAC address in the Layer 2 header of the received ARP packet matches the sender MAC address in the ARP header.

2. Range of values:

   None

dst-mac

When the dst-mac option is specified, the Switch checks whether the destination MAC address in the Layer 2 header of the received ARP packet matches the target MAC address in the ARP header. This inspection is performed on an ARP reply.

1. Default value when this parameter is omitted:

   When the dst-mac option is not specified, the Switch does not check whether the destination MAC address in the Layer 2 header of the received ARP packet matches the target MAC address in the ARP header.

2. Range of values:

   None

ip

This inspection item checks if the target IP address in the ARP header of the received ARP packet is within the following ranges:

- 1.0.0.0 to 126.255.255.255
- 128.0.0.0 to 223.255.255.255

This inspection is performed on an ARP reply only.

1. Default value when this parameter is omitted:

   The target IP address in the ARP header of the received ARP packet is not checked.

2. Range of values:

None

Default behavior

Additional dynamic ARP inspections 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

ip arp inspection vlan

ip dhcp snooping

ip dhcp snooping vlan

ip arp inspection vlan

Sets the VLAN used for dynamic ARP inspections when DHCP snooping is enabled on a Switch.

Syntax

To set information:

ip arp inspection vlan <*vlan id list*>

To change information:

ip arp inspection vlan {<*vlan id list*> | add <*vlan id list*> | remove <*vlan id list*>}

To delete information:

no ip arp inspection vlan

Input mode

`(config)`

Parameters

<*vlan id list*>

Sets the IDs of the VLANs used for dynamic ARP inspections.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

add <*vlan id list*>

Adds the IDs of VLANs that will be used for dynamic ARP inspection to the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

remove <*vlan id list*>

Removes the IDs of the VLANs used for dynamic ARP inspections from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

Default behavior

Dynamic ARP inspections are not used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A VLAN ID for which DHCP snooping is enabled must be set for this command.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping

Enables DHCP snooping on a Switch.

Syntax

To set information:

ip dhcp snooping

To delete information:

no ip dhcp snooping

Input mode

`(config)`

Parameters

None

Default behavior

DHCP snooping is not used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `qos-only` is set for the flow distribution pattern of the `fldm prefer` command, this command cannot be set. Similarly, if `standard` or `extended` is set for the flow detection extended mode, this command cannot be set.

Related commands

fldm prefer

ip dhcp snooping database url

Specifies where a binding database is to be saved.

Syntax

To set or change information:

ip dhcp snooping database url {flash | mc <*file name*>}

To delete information:

no ip dhcp snooping database url

Input mode

`(config)`

Parameters

{flash | mc <*file name*>}

Specifies where a binding database is to be saved.

flash

The database is saved to internal flash memory.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   flash

mc <*file name*>

The database is saved to a memory card.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*file name*>: A maximum of 64 characters can be set.

   Specify the name of a file on the memory card. If directories are created on a memory card by using an operation command, a maximum of 64 characters, including the directory name, can be set.

Default behavior

The binding database is not saved.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the save delay time set by using the `ip dhcp snooping database write-delay` command, any of the save events below causes the timer to start. When the timer expires, the binding database is saved.

- When terminal information is dynamically registered, updated, or deleted in a binding database
- When the `ip dhcp snooping database url` command is set (this includes changes to the save destination).
- When the `clear ip dhcp snooping binding` operation command is executed

If the Switch power is turned off before the timer expires, the binding database cannot be saved.

2. If the `no ip dhcp snooping database url` command is entered after the timer set by using the `ip dhcp snooping database write-delay` command has started, the binding database is not saved.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping database write-delay

Sets the maximum save delay time to be applied when a binding database is saved.

Syntax

To set or change information:

ip dhcp snooping database write-delay <*seconds*>

To delete information:

no ip dhcp snooping database write-delay

Input mode

(config)

Parameters

<*seconds*>

Sets the maximum save delay time to be applied when a binding database is saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1800 to 86400 (seconds)

Default behavior

For the maximum save delay time, 1800 seconds is set.

Impact on communication

None

When the change is applied

The setting takes effect at the next save event after the setting value has been changed.

Notes

1. For the save delay time set by using this command, any of the save events below causes the timer to start. When the timer expires, the binding database is saved.
   - When terminal information is dynamically registered, updated, or deleted in a binding database
   - When the `ip dhcp snooping database url` command is set (this includes changes to the save destination).
   - When the `clear ip dhcp snooping binding` operation command is executed

   If the Switch power is turned off before the timer expires, the binding database cannot be saved.
2. If the `no ip dhcp snooping database url` command is entered after the timer set by using the `ip dhcp snooping database write-delay` command has started, the binding database is not saved.

Related commands

ip dhcp snooping

ip dhcp snooping database url

ip dhcp snooping vlan

ip dhcp snooping information option allow-untrusted

Allows untrusted ports to receive DHCP packets that have the relay agent information option (Option 82).

Syntax

To set information:

ip dhcp snooping information option allow-untrusted

To delete information:

no ip dhcp snooping information option allow-untrusted

Input mode

(config)

Parameters

None

Default behavior

DHCP packets that have the relay agent information option are discarded.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip dhcp snooping

ip dhcp snooping limit rate

Sets the maximum DHCP packet reception rate (the number of DHCP packets that can be received per second) per Switch. DHCP packets exceeding the reception rate are discarded. The actual maximum reception rate is the sum of that set by this command and that set by the `ip arp inspection limit rate` command. The number of packets that can be received is the total number of DHCP packets and ARP packets.

Syntax

To set or change information:

ip dhcp snooping limit rate <*packet/s*>

To delete information:

no ip dhcp snooping limit rate

Input mode

`(config)`

Parameters

<*packet/s*>

Specify the number of DHCP packets that can be received per second.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 125 (packets/s)

Default behavior

The reception rate is not restricted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Values specified by using this command set the upper limit for the number of received packets, but do not guarantee operation with the specified value.

Related commands

ip dhcp snooping

ip dhcp snooping logging enable

Enables the output of DHCP snooping operation log information to a syslog server.

Syntax

To set information:

ip dhcp snooping logging enable

To delete information:

no ip dhcp snooping logging enable

Input mode

(config)

Parameters

None

Default behavior

Operation log information is not output to a syslog server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip dhcp snooping

ip dhcp snooping loglevel

Specifies the level of messages to be logged in a DHCP snooping operation log. Use the `show ip dhcp snooping logging` operation command to display the logged messages.

Syntax

To set or change information:

ip dhcp snooping loglevel {error | warning | notice | info}

To delete information:

no ip dhcp snooping loglevel

Input mode

`(config)`

Parameters

{error | warning | notice | info}

error

Only error-level log messages are logged. Only software errors are logged.

warning

Error-level and warning-level log messages are logged. Detected error information, such as information of an invalid packet, is logged.

notice

Error-, warning-, and notice-level log messages are logged. Information about detected unauthorized servers is logged.

info

Error-, warning-, notice-, and info-level log messages are logged. Operation tracking information is also logged.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `error`, `warning`, `notice`, `info`

Default behavior

The level of messages to be logged in an operation log is `notice`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Logging of messages is enabled only when the `ip dhcp snooping` command is set.

Related commands

ip dhcp snooping

ip dhcp snooping trust

Sets whether the interface is a trusted port or an untrusted port.

Syntax

To set information:

ip dhcp snooping trust

To delete information:

no ip dhcp snooping trust

Input mode

(config-if)

Parameters

None

Default behavior

The applicable interface operates as an untrusted port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. On an interface on which this command is set, if the interface is accommodated in the VLAN where DHCP snooping is enabled, the inspection of DHCP packets is not performed.

Related commands

ip dhcp snooping

ip dhcp snooping verify mac-address

Sets whether to check if the source MAC address of DHCP packets received from an untrusted port matches the client hardware addresses in the DHCP packet.

Syntax

To set information:

no ip dhcp snooping verify mac-address

To delete information:

ip dhcp snooping verify mac-address

Input mode

(config)

Parameters

None

Default behavior

The source MAC address and the client hardware address are checked to see if they match.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If this command is not set, MAC addresses are checked, so the DHCP relay agent cannot connect to an untrusted port. (This occurs because the source MAC address in the packets that passed through the DHCP relay agent has been changed.)

Related commands

ip dhcp snooping

ip dhcp snooping vlan

Enables DHCP snooping in a VLAN. DHCP snooping is disabled if it is not set by using this command.

Syntax

To set information:

ip dhcp snooping vlan <*vlan id list*>

To change information:

ip dhcp snooping vlan {<*vlan id list*> | add <*vlan id list*> | remove <*vlan id list*>}

To delete information:

no ip dhcp snooping vlan

Input mode

```
(config)
```

Parameters

<*vlan id list*>

Specify the IDs of VLANs on which DHCP snooping is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

add <*vlan id list*>

Adds, to the VLAN list, the IDs of VLANs on which DHCP snooping is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

remove <*vlan id list*>

Deletes, from the VLAN list, the IDs of VLANs on which DHCP snooping is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

Default behavior

DHCP snooping is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. DHCP snooping is not valid in a VLAN in which this command has not been set.

Related commands

ip dhcp snooping

ip source binding

Sets a static entry to the binding database.

Syntax

To set information:

ip source binding <*mac address*> vlan <*vlan id*> <*ip address*> interface <*interface type*> <*interface number*>

To delete information:

no ip source binding <*mac address*> vlan <*vlan id*> <*ip address*> interface <*interface type*> <*interface number*>

Input mode

```
(config)
```

Parameters

<*mac-address*>

Sets the MAC address of a terminal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to ffff.ffff.ffff

<*vlan id*>

Sets the ID of a VLAN to which the terminal is connected.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

<*ip address*>

Sets the IP address of the terminal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

interface <*interface type*> <*interface number*>

Sets the number of the interface to which the terminal is connected.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*interface type*> <*interface number*>, the following values can be set:

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

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

- port-channel <*channel group number*>

For details about the valid setting range of <*nif no.*>/<*port no.*> and <*channel group number*>, 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. If, when entries are set, the number of binding database entries, including dynamic entries, exceeds the maximum number of entries, the entries cannot be registered in the binding database.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip verify source

Set this command to use the terminal filter based on the DHCP snooping binding database.

The terminal filter is functionality used to filter the packets of unregistered source IP and MAC addresses.

Syntax

To set or change information:

ip verify source [{port-security | mac-only}]

To delete information:

no ip verify source

Input mode

(config-if)

Parameters

{port-security | mac-only}

Sets a terminal filter condition.

port-security

Applies the terminal filter to both the source IP and the source MAC addresses.

mac-only

Applies the terminal filter only to source MAC addresses.

1. Default value when this parameter is omitted:

   The terminal filter is applied only to source IP addresses.

2. Range of values:

   port-security, mac-only

Default behavior

The terminal filter is not applied.

Impact on communication

If the terminal filter is applied, packets from the terminals that are not registered in the binding database are discarded regardless of the VLAN.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Terminal filters are disabled on trusted ports even when this command is set.
2. If this command is set when DHCP snooping is enabled, terminal filters are enabled even in a VLAN for which DHCP snooping is disabled.

Related commands

ip dhcp snooping

ip dhcp snooping trust

ip dhcp snooping vlan

ip source binding

Chapter 14. Redundancy of Power Supplies (PSs)

power redundancy-mode

power redundancy-mode

Sets whether to display a message notifying that the redundant power supply has not been implemented.

Syntax

To set information:

power redundancy-mode redundancy-check

To delete information:

no power redundancy-mode

Input mode

```
(config)
```

Parameters

redundancy-check

Checks whether the redundant power supply has been implemented.

If the redundant power supply has not been implemented, the Switch displays a message notifying that the redundant power supply has not been implemented.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The Switch does not check whether the redundant power supply has been implemented.

Even if the redundant power supply has not been implemented, the Switch does not display a message notifying that the redundant power supply has not been implemented.

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

15. Redundancy of BSUs [AX6700S]

redundancy bsu-load-balancing [AX6700S]

Sets the load balancing method for packet transfer.

Syntax

To set information:

redundancy bsu-load-balancing smac

To delete information:

no redundancy bsu-load-balancing

Input mode

(config)

Parameters

smac

Selects the BSUs to which to assign the received packets based on source MAC addresses. This method is effective in environments where there are many source MAC addresses in the forwarded packets. For details, see *18. Redundancy of BSUs [AX6700S]* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

Default behavior

The BSUs to which to assign the received packets are selected based on the ports where the packets are received.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

If you set this parameter, make sure you save the configuration and restart the Switch. The new setting values do not take effect until the Switch is restarted.

Notes

1. After changing this setting, do not restart BSUs and NIFs before restarting the Switch.
2. This command is used together with the `redundancy bsu-mode fixed` and `no system recovery` commands.
3. This command can be set if the `power-control`, `schedule-power-control mode`, `schedule-power-control max-bsu`, `schedule-power-control standby-bsu`, `schedule-power-control time-range`, and `adaptive-power-control enable` commands have not been set.
4. When this command is used, do not use the QoS bandwidth monitoring functionality or the storm control functionality.

Related commands

redundancy bsu-mode

no system recovery

redundancy bsu-mode [AX6700S]

Sets the operating mode of the BSU.

Syntax

To set information:

redundancy bsu-mode fixed

To delete information:

no redundancy bsu-mode

Input mode

(config)

Parameters

fixed

Specifies fixed mode. In this mode, only communications that use the failed BSU are disabled, without affecting communications that use the other normal BSUs. Communications that use the failed BSU result in communication failures. For details, see *18. Redundancy of BSUs [AX6700S]* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

Default behavior

Even if a BSU is blocked or fails, communications continue by using other normal BSUs.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

If you set this parameter, make sure you save the configuration and restart the Switch. The new setting values do not take effect until the Switch is restarted.

Notes

1. After changing this setting, do not restart BSUs and NIFs before restarting the Switch.
2. This command is used together with the `redundancy bsu-load-balancing smac` and `no system recovery` commands.
3. This command can be set if the `power-control`, `schedule-power-control mode`, `schedule-power-control max-bsu`, `schedule-power-control standby-bsu`, `schedule-power-control time-range`, and `adaptive-power-control enable` commands have not been set.
4. If this command is set, BSUs exceeding the number of BSUs set by the `redundancy max-bsu` command are not started.

Related commands

no system recovery

redundancy bsu-load-balancing smac

redundancy max-bsu [AX6700S]

Sets the number of BSUs to operate.

Syntax

To set or change information:

redundancy max-bsu <*max bsu*>

To delete information:

no redundancy max-bsu

Input mode

`(config)`

Parameters

<*max bsu*>

Sets the number of active PSPs. Having more active PSPs can increase packet transfer performance. For details, see *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3

Default behavior

Three BSUs operate.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. During scheduled operation of the power saving functionality, the Switch operates according to the configuration of the `schedule-power-control max-bsu` command.
2. During the traffic-based power saving operation, the Switch operates according to the configuration of the `adaptive-power-control max-bsu` command.
3. To operate all BSUs as active BSUs, set the number of implemented BSUs for the configuration parameter.

Related commands

None

redundancy standby-bsu [AX6700S]

Sets the mode for the standby BSU.

Syntax

To set or change information:

redundancy standby-bsu {hot | cold | cold2}

To delete information:

no redundancy standby-bsu

Input mode

`(config)`

Parameters

{hot | cold | cold2}

hot

Powers on the standby BSU, and switches between the active and standby BSUs if a failure occurs.

cold

Partially powering off the standby BSU allows you to reduce its power consumption. If a failure occurs in an active BSU, the standby BSU starts automatically, and the BSUs are switched. Note that the switching takes time because the standby BSU is started when the switching occurs.

cold2

Fully powering off the standby BSU allows you to reduce its power consumption to almost zero. If a failure occurs in an active BSU, the standby BSU starts automatically, and the BSUs are switched. Note that the switching takes time because the standby BSU is started when the switching occurs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `hot`, `cold`, or `cold2`

Default behavior

The standby BSU is powered on, and the BSUs are switched instantly if a failure occurs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The `cold` parameter in this command can be set if the `schedule-power-control mode`, `schedule-power-control max-bsu`, `schedule-power-control standby-bsu`, `schedule-power-control time-range`, and `adaptive-power-control enable` commands have not been set.

2. During scheduled operation of the power saving functionality, the Switch operates according to the configuration of the `schedule-power-control standby-bsu` command.
3. During traffic-based power saving operation, the Switch operates according to the configuration of the `adaptive-power-control standby-bsu` command.

Related commands

None

Chapter

16. Redundancy of PSPs [AX6600S]

redundancy max-psp [AX6600S]
redundancy standby-psp [AX6600S]

redundancy max-psp [AX6600S]

Sets the number of PSPs to operate.

Syntax

To set or change information:

redundancy max-psp <*max psp*>

To delete information:

no redundancy max-psp

Input mode

`(config)`

Parameters

<*max psp*>

Sets the number of active PSPs. Having more active PSPs can increase packet transfer performance.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 2

Default behavior

All operating PSPs are set as active PSPs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. During scheduled operation of the power saving functionality, the Switch operates according to the configuration of the `schedule-power-control max-psp` command.
2. During traffic-based power saving operation, the Switch operates according to the configuration of the `adaptive-power-control max-psp` command.

Related commands

None

redundancy standby-psp [AX6600S]

Sets the mode for the standby PSP.

Syntax

To set or change information:

redundancy standby-psp {hot | cold2}

To delete information:

no redundancy standby-psp

Input mode

(config)

Parameters

{hot | cold2}

hot

The standby PSP is powered on, and the PSPs are switched instantly if a failure occurs.

cold2

Fully powering off the standby PSP allows you to reduce its power consumption to almost zero. If a failure occurs in an active PSP, the standby PSP starts automatically, and the PSPs are switched. Note that the switching takes time because the standby PSP is started when the switching occurs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   hot, cold2

Default behavior

The standby PSP is powered on, and the PSPs are switched instantly if a failure occurs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. During scheduled operation of the power saving functionality, the Switch operates according to the configuration of the `schedule-power-control standby-psp` command.
2. During traffic-based power saving operation, the Switch operates according to the configuration of the `adaptive-power-control standby-psp` command.

Related commands

None

Chapter

17. NIF Redundancy Control [AX6700S] [AX6600S]

redundancy nif-group max-standby-nif [AX6700S] [AX6600S]
redundancy nif-group nif priority [AX6700S] [AX6600S]

redundancy nif-group max-standby-nif [AX6700S] [AX6600S]

Specifies a NIF redundancy group, and sets the maximum number of NIFs that are placed in standby status in the group.

Syntax

To set or change information:

redundancy nif-group <*nif group no.*> max-standby-nif <*max standby nif*>

To delete information:

no redundancy nif-group <*nif group no.*> max-standby-nif

Input mode

`(config)`

Parameters

<*nif group no.*>

Specifies a NIF redundancy group number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4

<*max standby nif*>

Specifies the maximum number of NIFs that are placed in standby status in the NIF redundancy group. If the number of active NIFs in the NIF redundancy group exceeds the number of NIFs specified by this command, the specified number of NIFs are placed in standby status. The NIFs that meet the following conditions are selected to be placed in standby status:

- Lower priority NIFs set by the `redundancy nif-group nif priority` command
- If the priority is the same, a NIF with a larger NIF number

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 1

Default behavior

All active NIFs in the NIF redundancy group are placed in standby status.

Impact on communication

If some active NIFs are placed in standby status due to the NIF redundancy control functionality, communications that were using these NIFs (current standby NIFs) will stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a scheduled time range has been set by the `schedule-power-control time-range`

command, during the time range, the settings specified by this command are disabled and the Switch operates according to the settings specified by the `schedule-power-control redundancy nif-group max-standby-nif` command.

Related commands

redundancy nif-group nif priority

redundancy nif-group nif priority [AX6700S] [AX6600S]

Defines a NIF redundancy group and specifies the NIFs to be included in the group, with their target NIF priority. If the number of active NIFs in the NIF redundancy group exceeds the value set by the `redundancy nif-group max-standby-nif` command, lower priority NIFs in the same group, the number of which is specified by the `redundancy nif-group max-standby-nif` command, are placed in standby status.

Syntax

To set information:

redundancy nif-group <*nif group no.*> nif <*nif no.*> priority <*priority*>

To delete information:

no redundancy nif-group <*nif group no.*> nif <*nif no.*>

Input mode

`(config)`

Parameters

<*nif group no.*>

Specifies a NIF redundancy group number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4

nif <*nif no.*>

Specifies a NIF number to be included in the group.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See the range of <*nif no.*> in *Specifiable values for parameters*.

priority <*priority*>

Specifies the NIF priority in the group. The lower the value, the higher the priority.

This set value is used to select the NIFs to be placed in standby status by the NIF redundancy control functionality. The NIFs that meet the following conditions are selected to be placed in standby status:

- Lower priority NIFs according to the setting specified by this command
- If the priority is the same, a NIF with a larger NIF number

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8

Default behavior

The NIF redundancy group is not set.

Impact on communication

If some active NIFs are placed in standby status due to the NIF redundancy control functionality, communications that were using these NIFs (current standby NIFs) will stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One NIF can belong to only one NIF redundancy group.
2. Up to two NIFs can belong to one NIF redundancy group.
3. When configuring link aggregation, set it to static mode.

Related commands

redundancy nif-group max-standby-nif

schedule-power-control nif-group max-standby-nif

Chapter 18. GSRP

advertise-holdtime
advertise-interval
backup-lock
flush-request-count
gsrp
gsrp-vlan
gsrp direct-link
gsrp exception-port
gsrp limit-control
gsrp no-flush-port
gsrp reset-flush-port
layer3-redundancy
no-neighbor-to-master
port-up-delay
reset-flush-time
selection-pattern
vlan-group disable
vlan-group priority
vlan-group vlan

advertise-holdtime

Specifies the retention time of received GSRP Advertise frames in seconds. If the retention time elapses before any GSRP Advertise frames are received, the Switch operates as follows:

In master status:

Maintains master status.

In backup status:

Changes to backup status (neighbor unknown) because the partner switch in master status cannot be recognized.

Syntax

To set or change information:

advertise-holdtime <*seconds*>

To delete information:

no advertise-holdtime

Input mode

`(config-gsrp)`

Parameters

<*seconds*>

Specifies the retention time of received GSRP Advertise frames in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 120

Default behavior

The retention time of the received GSRP Advertise frames is 5 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For `advertise-holdtime`, specify a value greater than `advertise-interval`. If you specify a value equal to or less than `advertise-interval` for `advertise-holdtime`, the Switch detects a timeout for receiving GSRP Advertise frames.

Related commands

None

advertise-interval

Sets the sending interval for GSRP Advertise frames.

Syntax

To set or change information:

advertise-interval <*seconds*>

To delete information:

no advertise-interval

Input mode

`(config-gsrp)`

Parameters

<*seconds*>

Specifies the sending interval for GSRP Advertise frames in seconds. This interval can be specified in 0.5 second increments.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0.5 to 60

Default behavior

The sending interval for GSRP Advertise frames is 1 second.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For `advertise-holdtime`, specify a value greater than `advertise-interval`. If you specify a value equal to or less than `advertise-interval` for `advertise-holdtime`, the Switch detects a timeout for receiving GSRP Advertise frames.

Related commands

None

backup-lock

Fixes the GSRP status of the Switch to backup status.

Syntax

To set information:

backup-lock

To delete information:

no backup-lock

Input mode

(config-gsrp)

Parameters

None

Default behavior

None

Impact on communication

Communications are interrupted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

flush-request-count

Specifies the number of times GSRP Flush request frames are sent to neighboring switches to request the clearing of MAC address tables.

Syntax

To set or change information:

flush-request-count <*count*>

To delete information:

no flush-request-count

Input mode

```
(config-gsrp)
```

Parameters

<*count*>

Specifies the number of times that GSRP Flush request frames are sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The number of times that GSRP Flush request frames are sent is 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Multiple GSRP Flush request frames are sent, but the receiving Switch clears the MAC address table entries only once.

Related commands

None

gsrp

Sets GSRP-related items.

Syntax

To set information:

gsrp <*gsrp group id*>

To delete information:

no gsrp <*gsrp group id*>

Input mode

`(config)`

Parameters

<*gsrp group id*>

Sets a GSRP group ID. For GSRP switches that belong to the same GSRP group, specify the same GSRP group ID. Each GSRP group must have a unique number in the network. After this command is entered, the mode is changed to `config-gsrp` mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

Communications are interrupted. Even for the ports for which the `gsrp exception-port` command has been set, or for the ports that do not belong to any VLAN groups (when the `gsrp limit-control` command has been set), communications are interrupted temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting cannot work with Spanning Tree Protocol or VRRP.
2. The status of the ports that do not belong to the VLAN specified by the `vlan-group vlan` command depends on the functionality limiting GSRP control to VLAN-group VLANs, which is set by the `gsrp limit-control` command. If the functionality limiting GSRP control to VLAN-group VLANs is not set, the ports will be blocked.

Related commands

None

gsrp-vlan

Specifies a VLAN to be used as the GSRP-managed VLAN.

Syntax

To set or change information:

gsrp-vlan <*vlan id*>

To delete information:

no gsrp-vlan

Input mode

`(config-gsrp)`

Parameters

<*vlan id*>

Specifies the ID of the VLAN to be used as the GSRP-managed VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

The ID of the GSRP-managed VLAN is 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

vlan

gsrp direct-link

Configures the ports used for a direct link between switches.

Syntax

To set information:

gsrp <*gsrp group id*> direct-link

To delete information:

no gsrp <*gsrp group id*> direct-link

Input mode

`(config-if)`

Parameters

<*gsrp group id*>

Sets a GSRP group ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

direct-link

Configures the direct link ports.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Specify the ports that belong to the VLAN specified by the `gsrp-vlan` command. If the specified port does not belong to the VLAN, GSRP does not work.
2. This command cannot be set for the ports for which the `gsrp reset-flush-port` command or the `gsrp no-flush-port` command has been set.

Related commands

gsrp-vlan

gsrp exception-port

Configures a port not under GSRP control. The set port is always able to forward frames.

Syntax

To set information:

gsrp exception-port

To delete information:

no gsrp exception-port

Input mode

(config-if)

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

1. A loop might occur depending on the specified port or link aggregation because the specified port is always able to forward frames.

Related commands

None

gsrp limit-control

Enables the GSRP VLAN group-only control functionality.

If the functionality limiting GSRP control to VLAN-group VLANs is set by this command, only the VLANs that belong to any VLAN group are under GSRP control. The VLAN ports that do not belong to any VLAN group are able to forward frames.

Syntax

To set information:

gsrp limit-control

To delete information:

no gsrp limit-control

Input mode

(config)

Parameters

None

Default behavior

All VLANs are controlled by GSRP regardless whether to belong to any VLAN group. Therefore, the VLAN ports that do not belong to any VLAN group are blocked.

Impact on communication

For the VLAN ports that do not belong to any VLAN group and that are not controlled by GSRP, communications are interrupted temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

vlan-group vlan

gsrp no-flush-port

Specifies a port that does not send GSRP Flush request frames.

Syntax

To set information:

gsrp <*gsrp group id*> no-flush-port

To delete information:

no gsrp <*gsrp group id*> no-flush-port

Input mode

`(config-if)`

Parameters

<*gsrp group id*>

Sets a GSRP group ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

no-flush-port

Sets the functionality of not sending GSRP Flush request frames.

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 the ports for which the `gsrp direct-link` command or the `gsrp reset-flush-port` command has been set.
2. This command setting cannot be applied to the ports for which the `axrp-ring-port` command has been set.

Related commands

None

gsrp reset-flush-port

Specifies a port on which port resetting is used.

Syntax

To set information:

gsrp <*gsrp group id*> reset-flush-port

To delete information:

no gsrp <*gsrp group id*> reset-flush-port

Input mode

`(config-if)`

Parameters

<*gsrp group id*>

Sets a GSRP group ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

reset-flush-port

Configures port resetting.

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 the ports for which the `gsrp direct-link` command or the `gsrp no-flush-port` command has been set.
2. This command setting cannot be applied to the ports for which the `axrp-ring-port` command has been set.

Related commands

None

layer3-redundancy

Enables the Layer 3 redundancy switching functionality for the target GSRP group.

Syntax

To set information:

layer3-redundancy

To delete information:

no layer3-redundancy

Input mode

(config-gsrp)

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

1. This command can be set only when the GSRP group ID is 1 to 4.
2. To use the Layer 3 redundancy switching functionality, also set this command for the partner switch.
3. The setting of the IPv4 address and IPv6 address for the VLAN that operates under GSRP control must be the same between this Switch and the partner switch.

Related commands

None

no-neighbor-to-master

To allow a GSRP switch in backup (neighbor unknown) status to take over the master, you can choose whether to perform manual switchover (by entering a command that changes the Switch status to master status) or automatic switchover (when a direct-link port failure is detected).

Syntax

To set or change information:

no-neighbor-to-master { manual | direct-down [forced-shift-time <*seconds*>] }

To delete information:

no no-neighbor-to-master

Input mode

`(config-gsrp)`

Parameters

{ manual | direct-down [forced-shift-time <*seconds*>] }

Specifies the operation mode in which a GSRP switch changes from the backup (neighbor unknown) status to master status.

manual

The Switch keeps waiting in backup (neighbor unknown) status until GSRP Advertise frames are received, or until a command that changes the Switch status to master status is entered.

direct-down [forced-shift-time <*seconds*>]

If all ports specified for a direct link are in failed status, the Switch starts operating as the master. To make a GSRP switch automatically run as the master when it is independently started by using the functionality for switchover to master status by an independently started GSRP switch, set the `forced-shift-time` parameter.

- forced-shift-time <*seconds*>

  For <*seconds*>, specify the time (in seconds) to wait until the GSRP switch automatically starts operating as the master when it is independently started. You can specify the time in the range from 0 to 3600 seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `manual` or `direct-down`.

   To make a GSRP switch run automatically as the master when it is independently started, set both `forced-shift-time` and the time to wait until the GSRP switch automatically starts operating as the master.

Default behavior

The default way of switching over from backup (neighbor unknown) status to master status is manual switchover.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `direct-down` is set for the operation mode in which a GSRP switch changes from backup (neighbor unknown) status to master status, the Switch starts operating as the master when all ports specified for a direct link are in a fault state.

   However, after the operations below, if GSRP Advertise frames are never received on the ports specified for a direct link, the Switch keeps waiting in backup (neighbor unknown) status. If you want to make the Switch run as the master in this case, enter a command to change the Switch status to master status (the `set gsrp master` operation command).

   - Starting the switch
   - Switching the system
   - Executing the `restart vlan` operation command
   - Executing the `restart gsrp` operation command
   - Specifying `direct-down` in the `no-neighbor-to-master` command
   - Setting direct link ports by using the `gsrp direct-link` command
   - Applying the setting to the running configuration by using the `copy` operation command
   - Executing the `inactivate bsu` operation command, which inactivates all BSUs [AX6700S]

2. A GSRP switch automatically changes from backup status to master status (by using the functionality for switchover to master status by an independently started GSRP switch) only once when it is independently started. However, this switchover is performed again when any of the following operations is performed:

   - Switching the system
   - Executing the `restart vlan` operation command
   - Executing the `restart gsrp` operation command
   - Applying the setting to the running configuration by using the `copy` operation command
   - Executing the `activate bsu` operation command, which activates the first BSU [AX6700S]

Related commands

None

port-up-delay

Specifies a time for delaying the inclusion of ports that have come up in the number of active ports. GSRP uses the number of active ports as the condition for selecting the master and backup switches. If ports become unstable (for example, ports are frequently enabled and disabled), the number of active ports changes frequently, leading to repeated switchovers between the master and backup switches. If ports are unstable, use this command to specify a delay time to prevent unnecessary switchovers.

To include the ports that have come up during the delay time in the number of active port, enter a command for including ports in the number of active ports (the `clear gsrp port-up-delay` operation command).

Syntax

To set or change information:

port-up-delay <*seconds*>

To delete information:

no port-up-delay

Input mode

`(config-gsrp)`

Parameters

<*seconds*>

Specifies a time (in seconds) for delaying the inclusion of ports that have come up in the number of active ports. If you specify `infinity`, the delay time is unlimited and the ports that come up are not automatically included in the number of active ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 43200, or `infinity`

Default behavior

Ports that come up are immediately included in the number of active ports (delay time is 0 seconds).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

reset-flush-time

Sets the port-down time to be applied when port resetting is used.

Syntax

To set or change information:

reset-flush-time <*seconds*>

To delete information:

no reset-flush-time

Input mode

`(config-gsrp)`

Parameters

<*seconds*>

Specifies the port-down time (in seconds) to be applied when port resetting is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The port-down time is 3 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is valid for all the ports for which the `gsrp reset-flush-port` command has been set.

Related commands

None

selection-pattern

Specifies the precedence of the conditions for selecting the master and backup GSRP switches (number of active ports, priority, and switch MAC address).

Syntax

To set or change information:

selection-pattern { ports-priority-mac | priority-ports-mac }

To delete information:

no selection-pattern

Input mode

`(config-gsrp)`

Parameters

{ ports-priority-mac | priority-ports-mac }

Specifies the precedence of the conditions for selecting the master and backup GSRP switches.

ports-priority-mac

The number of active ports, the priority, and the MAC address of the switch are selected in that order.

priority-ports-mac

The priority, the number of active ports, and the MAC address of the switch are selected in that order.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `ports-priority-mac` or `priority-ports-mac`

Default behavior

The number of active ports, the priority, and the MAC address of the switch are selected in that order (`ports-priority-mac`).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

vlan-group disable

Disables the GSRP functionality for the specified VLAN group.

Syntax

To set information:

vlan-group <*vlan group id*> disable

To delete information:

no vlan-group <*vlan group id*> disable

Input mode

```
(config-gsrp)
```

Parameters

<*vlan group id*>

Specifies the ID of a VLAN group that operates under GSRP control.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 128

Default behavior

The GSRP functionality is enabled for each VLAN group.

Impact on communication

Communications are interrupted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

vlan-group priority

Sets the priority of a VLAN group that operates under GSRP control.

Syntax

To set or change information:

vlan-group <*vlan group id*> priority <*priority*>

To delete information:

no vlan-group <*vlan group id*> priority

Input mode

```
(config-gsrp)
```

Parameters

<*vlan group id*>

Specifies the ID of a VLAN group that operates under GSRP control.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 128

priority <*priority*>

Specifies the priority of the VLAN group. The larger the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 255

Default behavior

The priority of a VLAN group is 100.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

vlan-group vlan

Sets VLANs participating a VLAN group that operates under GSRP control.

Syntax

To set information:

vlan-group <*vlan group id*> vlan <*vlan id list*>

To change information:

vlan-group <*vlan group id*> vlan { <*vlan id list*> | add <*vlan id list*> | remove <*vlan id list*> }

To delete information:

no vlan-group <*vlan group id*> vlan

Input mode

```
(config-gsrp)
```

Parameters

<*vlan group id*>

Specifies the ID of a VLAN group that operates under GSRP control.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 128

vlan <*vlan id list*>

Specifies the IDs of the VLANs participating in the VLAN group. If you specify multiple VLAN IDs, you can specify a range.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

add <*vlan id list*>

Adds a VLAN to the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

remove <*vlan id list*>

Removes a VLAN from the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable 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. If Ring Protocol and GSRP are used together, the same value cannot be used for the VLAN mapping ID and the GSRP VLAN group ID if the value is in the following range:

   IDs for which concurrent use is not allowed: 108 to 128

2. If GSRP and VRF are used together (by setting the `vrf mode` command with the `gsrp-enable-ipv4-ipv6` parameter specified), the number of VLANs belonging to one VLAN group must be no more than 250. [OP-NPAR]

Related commands

vlan

Chapter 19. VRRP

track check-reply-interface

Sets whether to check if the interface that received a reply to a VRRP polling request matches the interface that sent the VRRP polling request.

Syntax

To set information:

track <*track number*> check-reply-interface

To delete information:

no track <*track number*> check-reply-interface

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

Whether the interface that received a reply to a VRRP polling request matches the interface that sent the VRRP polling request is not checked.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.

Related commands

ip address

track interface

track ip route

vrrp ip

vrrp track

track check-status-interval

Sets the interval for VRRP polling operations.

Syntax

To set or change information:

track <*track number*> check-status-interval <*seconds*>

To delete information:

no track <*track number*> check-status-interval

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*seconds*>

Specifies the interval (in seconds) for VRRP polling operations. If VRRP polling is performed at a set interval and then packets are lost or recovered, it is checked whether an interface fault has occurred or whether the interface has recovered from a fault. For the track specified in this command, the `track interface` command must be set with the `ip routing` option specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

VRRP polling is performed every 6 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.

Related commands

interface vlan

ip address

track interface

track ip route

vrrp ip

vrrp track

track check-trial-times

Sets the number of retries for VRRP polling to be attempted while checking whether an interface fault has occurred or whether the interface has recovered from a fault.

Syntax

To set or change information:

track <*track number*> check-trial-times <*count*>

To delete information:

no track <*track number*> check-trial-times

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*count*>

Specifies the number of retries for VRRP polling to be attempted while checking whether an interface fault has occurred or whether the interface has recovered from a fault. For the track specified in this command, the `track interface` command must be set with the `ip routing` option specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The number of retries for VRRP polling to be attempted while checking whether an interface fault has occurred or whether the interface has recovered from a fault is set to 4 times.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.

Related commands

interface vlan

ip address
track interface
track ip route
vrrp ip
vrrp track

track failure-detection-interval

Sets the interval for VRRP polling attempts to be performed during failure verification relating to VRRP polling.

Syntax

To set or change information:

track <*track number*> failure-detection-interval <*seconds*>

To delete information:

no track <*track number*> failure-detection-interval

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*seconds*>

Specifies the interval (in seconds) for VRRP polling attempts to be performed during failure verification. For the track specified in this command, the `track interface` command must be set with the `ip routing` option specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

The interval for VRRP polling attempts during failure verification is set to 2 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.

Related commands

ip address

track interface

track ip route

vrrp ip

vrrp track

track failure-detection-times

Sets the maximum number of retries for VRRP polling to be successful during failure verification.

Syntax

To set or change information:

track <*track number*> failure-detection-times <*count*>

To delete information:

no track <*track number*> failure-detection-times

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*count*>

Sets the maximum number of retries for VRRP polling to be successful during failure verification. Note that this value must be equal to or smaller than the `check-trial-times` value. For the track specified in this command, the `track interface` command must be set with the `ip routing` option specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of retries for VRRP polling to be successful during failure verification is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.

Related commands

ip address

track interface

track ip route

vrrp ip

vrrp track

track interface

Specifies the interface used for failure monitoring. When you set VLAN failure monitoring, use this command to set whether to perform VRRP polling or interface failure monitoring.

Syntax

To set information:

track <*track number*> interface { vlan <*vlan id*> { line-protocol | ip routing } | <*interface type*> <*interface number*> line-protocol }

To change information:

track <*track number*> interface { vlan <*vlan id*> | <*interface type*> <*interface number*> } line-protocol

track <*track number*> interface vlan <*vlan id*> ip-routing

To delete information:

no track <*track number*> interface

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

vlan <*vlan id*>

Specify the ID of the VLAN for which failure monitoring is to be performed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*vlan id*>, specify the VLAN ID set by the `interface vlan` command.

{ line-protocol | ip routing }

line-protocol

Performs interface failure monitoring.

ip routing

Performs VRRP polling.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `line-protocol` or `ip routing`

<interface type> <interface number>

Specifies the interface for failure monitoring.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For *<interface type> <interface number>*, the following values can be specified:

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

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

   For details about the valid setting range of *<nif no.>*/*<port no.>*, see *Specifiable values for parameters*.

   - port-channel *<channel group number>*

   For details about the valid setting range of *<channel group number>*, 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. The maximum number of tracks that can be set per switch is 255.
2. An IP address must be assigned to the VLAN interface for failure monitoring.
3. When changing the parameter for a track from the `ip routing` parameter to the `line-protocol` parameter, first delete this command, and then set the command again. Similarly, when changing the parameter for a track from the `line-protocol` parameter to the `ip routing` parameter, first delete this command, and then set the command again.
4. When specifying the `ip routing parameter`, set the destination address used for VRRP polling by using the `track ip route` command. If the destination address is not set, interface failure monitoring is performed.

Related commands

ip address

track ip route

vrrp ip

vrrp track

track ip route

Sets the destination address for VRRP polling.

Syntax

To set or change information:

track <*track number*> ip route {<*ip address*> | <*ipv6 address*>} reachability

To delete information:

no track <*track number*> ip route [{<*ip address*> | <*ipv6 address*>} reachability]

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

{<*ip address*> | <*ipv6 address*>} reachability

Specifies the destination address for VRRP polling in IPv4 format or IPv6 format. For the track specified in this command, the `track interface` command must be set with the `ip routing` option specified. The route to the destination IP address must be resolvable by using a routing protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   IPv4 address and `reachability`, or IPv6 address and `reachability`

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 setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.
2. Set the destination IP address for VRRP polling to the same address family as the IP address of the VLAN specified in the `track interface` command.
3. When changing the address family of the destination address for VRRP polling, first delete the configuration, and then set the configuration again.

Related commands

ip address

track interface

vrrp ip

vrrp track

track recovery-detection-interval

Sets the interval for VRRP polling attempts to be performed during failure recovery verification relating to VRRP polling.

Syntax

To set or change information:

track <*track number*> recovery-detection-interval <*seconds*>

To delete information:

no track <*track number*> recovery-detection-interval [<*seconds*>]

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*seconds*>

Specifies the interval (in seconds) for VRRP polling attempts to be performed during failure recovery verification. For the track specified in this command, the `track interface` command must be set with the `ip routing` option specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

The interval for VRRP polling attempts during failure recovery verification is set to 2 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.

Related commands

ip address

track interface

track ip route

vrrp ip

vrrp track

track recovery-detection-times

Sets the maximum number of retries for VRRP polling to be successful during failure recovery verification relating to VRRP polling.

Syntax

To set or change information:

track <*track number*> recovery-detection-times <*count*>

To delete information:

no track <*track number*> recovery-detection-times

Input mode

`(config)`

Parameters

<*track number*>

Specifies the number of the track to which the setting is to be saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*count*>

Specifies the maximum number of retries for VRRP polling to be successful during failure recovery verification. Note that this value must be equal to or smaller than the `check-trial-times` value. For the track specified in this command, the `track interface` command must be set with the `ip routing` option specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of retries for VRRP polling to be successful during failure recovery verification is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command setting is valid only for the tracks for which the `track interface` command is set with the `ip routing` option specified.

Related commands

ip address

track interface

track ip route

vrrp ip

vrrp track

vrrp accept

Configures a virtual router in accept mode. If access mode is enabled by this command, a virtual router in the master state can receive IP packets even if the router is not the owner of the IP address.

Syntax

To set information:

vrrp <*vrid*> accept

To delete information:

no vrrp <*vrid*> accept

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

Accept mode is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If accept mode is enabled for the IP address owner, the virtual router acts as the IP address owner.
2. This command can be specified only when both the real IP address and the virtual IP address exist on the same network.
3. If a real IP address that is the same as the virtual IP address of VRRP for which accept mode is enabled is set on the same network, these IP addresses are duplicated.

   Also, if the virtual IP address and the real IP address for the IP address owner are set on the same network, these IP addresses are duplicated, as same as when accept mode is enabled.
4. If duplicated IPv6 address is detected, sending and receiving of IP packets is no longer available. In such a case, check the configuration, and try to place the interface in Up or Down state (by using the `activate/inactivate` operation command).

Related commands

None

vrrp authentication

Sets the password used for advertisement packet authentication on a virtual router.

Syntax

To set or change information:

vrrp <*vrid*> authentication <*text*>

To delete information:

no vrrp <*vrid*> authentication

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*text*>

Specifies the password (SIMPLE TEXT PASSWORD) used for advertisement packet authentication.

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 8 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

No password is set. Advertisement packet authentication is not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is invalid when the `vrrp ietf-ipv6-spec-07-mode` command or the `vrrp ietf-unified-spec-02-mode` command has been set.
2. This setting is invalid when the `vrrp follow` command has been set.

Related commands

None

vrrp follow

Sets a virtual router to the follower virtual router by specifying the primary virtual router. The tracking functionality, the priority setting, the PREEMPT mode setting, the VRRP operation mode setting, and the setting of the sending interval for advertisement packets that have been set for the follower virtual router are disabled. The follower virtual router follows the operation of the primary virtual router.

Syntax

To set or change information:

vrrp <*vrid*> follow <*string*>

To delete information:

no vrrp <*vrid*> follow

Input mode

```
(config-if)
```

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*string*>

Specifies the primary virtual router name.

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 15 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

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 if the virtual router is the IP address owner.
2. This command cannot be set if the virtual router has been specified as the primary virtual

router for other virtual router. Also, for the primary virtual router name, you cannot specify the virtual router name or follower virtual router name of the router for which you are configuring the setting.

Related commands

vrrp name

vrrp-vlan

vrrp ietf-ipv6-spec-07-mode

Sets an IPv6 virtual router to operate in the mode according to `draft-ietf-vrrp-ipv6-spec-07`.

This command is valid when an IPv6 virtual router has been set.

Syntax

To set information:

vrrp <*vrid*> ietf-ipv6-spec-07-mode

To delete information:

no vrrp <*vrid*> ietf-ipv6-spec-07-mode

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

An IPv6 virtual router operates according to draft-ietf-vrrp-unified-spec-02 when the `vrrp ietf-unified-spec-02-mode` command is set, and operates according to draft-ietf-vrrp-ipv6-spec-02 when the `vrrp ietf-unified-spec-02-mode` command is not set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Setting this command also changes the format of advertisement packets. If this setting is not the same on all switches that establish VRRP, the state transitions in VRRP are not normally performed, allowing multiple master routers at the same time.
2. When this setting or another equivalent setting is performed for switches that establish VRRP, multiple master routers exist temporarily. After the settings for the switches are completed (as the same setting), only one master router is selected automatically.
3. This command cannot be set for a virtual router for which another VRRP operation mode is set.
4. When you enter this setting, if the setting value set by the `vrrp timers advertise` command exceeds 40, the interval of sending advertisement packets will be 1 second (default).

Related commands

ipv6 address

vrrp ipv6

vrrp ietf-unified-spec-02-mode

Sets a virtual router so that it operates according to draft-ietf-vrrp-unified-spec-02.

Syntax

To set information:

vrrp <*vrid*> ietf-unified-spec-02-mode

To delete information:

no vrrp <*vrid*> ietf-unified-spec-02-mode

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

An IPv4 virtual router operates according to RFC3768.

An IPv6 virtual router operates according to draft-ietf-vrrp-ipv6-spec-07 when the `vrrp ietf-ipv6-spec-07-mode` command is set, and operates according to draft-ietf-vrrp-ipv6-spec-02 when the `vrrp ietf-ipv6-spec-07-mode` command is not set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Setting this command also changes the format of advertisement packets. If this setting is not the same on all switches that establish VRRP, the state transitions in VRRP are not normally performed, allowing multiple master routers at the same time.
2. When this setting or another equivalent setting is performed for switches that establish VRRP, multiple master routers exist temporarily. After the settings for the switches are completed (as the same setting), only one master router is selected automatically.
3. This command cannot be set for a virtual router for which another VRRP operation mode is set.
4. When you enter this setting, if the setting value set by the `vrrp timers advertise` command exceeds 40, the interval of sending advertisement packets will be 1 second (default).
5. This setting is invalid when the `vrrp follow` command has been set.

Related commands

vrrp ietf-ipv6-spec-07-mode

vrrp ip

Assigns an IPv4 address to a virtual router.

Syntax

To set or change information:

vrrp <*vrid*> ip <*ip address*>

To delete information:

no vrrp <*vrid*> ip

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*ip address*>

Specifies the IP address of the virtual router.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   IPv4 address

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The maximum number of virtual routers (including both IPv4 virtual routers and IPv6 virtual routers) that can be set per switch is 255. You can increase this number to 4095 by using the group functionality to create follower virtual routers.
2. After an IP address is assigned to a virtual router by this command, the virtual router starts operating.
3. A virtual router for which the `vrrp follow` command has been set cannot be set as the address owner.

Related commands

ip address

vrrp ipv6

Assigns an IPv6 address to a virtual router.

Syntax

To set or change information:

vrrp <*vrid*> ipv6 <*ipv6 address*>

To delete information:

no vrrp <*vrid*> ipv6

Input mode

(config-if)

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*ipv6 address*>

Specifies the IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   IPv6 address

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The maximum number of virtual routers (including both IPv4 virtual routers and IPv6 virtual routers) that can be set per switch is 255. You can increase this number to 4095 by using the group functionality to create follower virtual routers.
2. After an IPv6 address is assigned to a virtual router by this command, the virtual router starts operating.

Related commands

ipv6 address

vrrp name

Sets a name for a virtual router.

Syntax

To set information:

vrrp <*vrid*> name <*string*>

To delete information:

no vrrp <*vrid*> name

Input mode

(config-if)

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*string*>

Specifies the primary virtual router name.

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 15 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

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A virtual router for which this command is set detects a failure by means of tracking functionality. When the priority of the virtual router is 0, the IP interface for which the virtual router is set is not brought down.

Related commands

vrrp follow

vrrp preempt

Sets automatic switchbacks for a virtual router. When automatic switchbacks are enabled, if a virtual router detects a master router that has a lower priority than itself, the virtual router automatically takes over the master router.

Syntax

To set information:

no vrrp <*vrid*> preempt

To delete information:

vrrp <*vrid*> preempt

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

Automatic switchbacks are enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `swap vrrp` command is executed when automatic switchback suppression has been set, the command has precedence and switchbacks are performed.
2. When a virtual router detects the down state of the master router, the virtual router takes over the master router regardless of the automatic switchback setting.
3. This setting is invalid when the `vrrp follow` command has been set.

Related commands

None

vrrp preempt delay

Sets a period of time for suppressing automatic switchbacks. If automatic switchbacks are enabled, switchback processing is suppressed for the specified period of time before it is processed.

Syntax

To set or change information:

vrrp <*vrid*> preempt delay <*seconds*>

To delete information:

no vrrp <*vrid*> preempt delay

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*seconds*>

Specifies a period of time (in seconds) for suppressing automatic switchbacks.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

The period of time for suppressing automatic switchbacks is set to 0 seconds. Automatic switchbacks are not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is invalid when the `vrrp follow` command has been set.

Related commands

None

vrrp priority

Sets the priority to a virtual router.

Syntax

To set or change information:

vrrp <*vrid*> priority <*priority*>

To delete information:

no vrrp <*vrid*> priority

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*priority*>

Specifies the priority of the virtual router. If the IP address of the virtual router is the same as the IP address specified for the VLAN (the virtual router is the owner of the IP address), the virtual router operates with the priority 255 regardless of this setting.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 (Low priority) to 254 (High priority)

Default behavior

If the IP address of the virtual router is the same as the IP address specified for the VLAN (the virtual router is the owner of the IP address), the priority of the virtual router is 255.

If the virtual router is not the owner of the IP address, the priority of the virtual router is 100.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is invalid when the `vrrp follow` command has been set.

Related commands

None

vrrp timers advertise

Sets the sending interval of advertisement packets to be sent by a virtual router.

Syntax

To set or change information:

vrrp <*vrid*> timers advertise <*seconds*>

vrrp <*vrid*> timers advertise msec <*milli seconds*>

To delete information:

no vrrp <*vrid*> timers advertise

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*seconds*>

Specifies the sending interval of advertisement packets in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

msec <*milli seconds*>

Specifies the sending interval (in milliseconds) of advertisement packets by 10 millisecond increments.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A multiple of 10 in the range from 250 to 40950

Default behavior

The sending interval of advertisement packets is set to 1 second.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `msec` parameter is not specified when the `vrrp ietf-ipv6-spec-07-mode` command or the `vrrp ietf-unified-spec-02-mode` command is set, setting of a value larger than 40 is ignored, and 1 second (default) is chosen as the sending interval.
2. The `msec` parameter is valid when the `vrrp ietf-ipv6-spec-07-mode` command or the `vrrp ietf-unified-spec-02-mode` command has been set.

   If the `msec` parameter is set, and both the `vrrp ietf-ipv6-spec-07-mode` command and the `vrrp ietf-unified-spec-02-mode` command are not set, 1 second (default) is chosen as the sending interval.
3. This setting is invalid when the `vrrp follow` command has been set.
4. When a virtual router is running on a VLAN on a channel group, if a small value is set for the `msec` parameter, multiple master routers might temporarily exist due to a line error of a port belonging to the channel group. After switching of the ports belonging to the channel group is completed, only one master router is chosen automatically.

Related commands

None

vrrp timers non-preempt-swap

Sets the switchback suppression time to be applied when switchback processing is performed while automatic switchbacks are suppressed.

Syntax

To set or change information:

vrrp <*vrid*> timers non-preempt-swap <*seconds*>

To delete information:

no vrrp <*vrid*> timers non-preempt-swap

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*seconds*>

Specify the switchback suppression time (in seconds) to be applied when switchback processing is performed while automatic switchbacks are suppressed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

The switchback suppression time to be applied when switchback processing is performed while automatic switchbacks are suppressed is set to 0 second. Switchbacks are not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is invalid when the `vrrp follow` command has been set.

Related commands

vrrp preempt

vrrp track

Configures the tracking functionality for a virtual router.

Syntax

To set or change information:

vrrp <*vrid*> track <*track number*> [{ priority | decrement } <*priority*>]

To delete information:

no vrrp <*vrid*> track <*track number*>

Input mode

`(config-if)`

Parameters

<*vrid*>

Specifies the virtual router ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

<*track number*>

Specifies the track number to be assigned to the virtual router for failure monitoring.

{priority | decrement} <*priority*>

This parameter defines the priority the tracking functionality sets to the virtual router during failure verification.

priority <*priority*>

Specify the priority the tracking functionality sets to the virtual router during failure verification, in the range 0 to 254. Also, specify a value smaller than the priority of the virtual router (set by using the `vrrp priority` command). If the specified value is equal to or larger than the priority of the virtual router, the setting specified by this command is ignored, and the priority 0 is used. If the virtual router is the owner of the IP address, the setting specified by this command is ignored, and the priority 0 is used. Only one track for which the `priority` parameter is specified can be set per virtual router.

decrement <*priority*>

Specify a value the tracking functionality subtracts from the current priority value of the virtual router during failure verification, in the range from 1 to 255. Multiple tracks for which the `decrement` parameter is specified can be registered per virtual router.

1. Default value when this parameter is omitted:

   The `decrement` parameter and the priority 255 are used.

2. Range of values:

   When `priority` <*priority*> is specified, the specifiable range for the priority is from 0 to 254.

   When `decrement` <*priority*> is specified, the specifiable range for the value to be subtracted from the priority value is from 1 to 255.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The number of tracks that can be assigned to a virtual router by using this command with the `priority` parameter specified is one per virtual router.
2. If you assigned a track to a virtual router by using this command with the `priority` parameter specified, and if you want to change the parameter to the `decrement` parameter, delete this command.
3. If you assigned a track to a virtual router by using this command with the `decrement` parameter specified, and if you want to change the parameter to the `priority` parameter, delete all the tracks assigned to the virtual router.
4. A virtual router for which this command is set detects a failure by means of tracking functionality. When the priority of the virtual router is 0, the IP interface for which the virtual router is set is brought down.
5. This setting is invalid when the `vrrp follow` command has been set.

Related commands

track interface

vrrp-vlan

Specifies a VLAN to be used as the VRRP-managed VLAN. If a virtual router set for the Switch is changed to the master, the virtual router sends Flush Request frames (which prompts clearing the MAC address table entries) to the VRRP-managed VLAN specified by this command.

Syntax

To set information:

vrrp-vlan <*vlan id*>

To delete information:

no vrrp-vlan

Input mode

`(config)`

Parameters

<*vlan id*>

Specifies the ID of the VLAN to be used as the VRRP-managed VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   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

vrrp ip

vrrp ipv6

vrrp follow

Chapter 20. IEEE 802.3ah/UDLD

efmoam active
efmoam disable
efmoam udld-detection-count

efmoam active

Sets the port to be monitored by the IEEE 802.3ah/OAM functionality to active mode.

Syntax

To set or change information:

efmoam active [udld]

To delete information:

no efmoam active

Input mode

(config-if)

Parameters

udld

Specifies that the port be monitored using the IEEE 802.3ah/UDLD functionality and enables the unidirectional link failure detection functionality.

1. Default value when this parameter is omitted:

   The unidirectional link failure detection functionality is not executed on the applicable port.

2. Range of values:

   udld

Default behavior

The applicable port operates in passive mode and does not detect a unidirectional link failure.

Impact on communication

If this functionality is enabled and a line failure is detected, the applicable port is deactivated.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the udld parameter is not set on both connected ports, link failures cannot be detected by using this functionality.

Related commands

None

efmoam disable

Enables or disables the IEEE 802.3ah/OAM functionality on a switch.

To disable the IEEE 802.3ah/OAM functionality, set the `efmoam disable` command.

To enable the IEEE 802.3ah/OAM functionality again, set the `no efmoam disable` command.

In passive mode, the send process starts when an OAMPDU from the active mode is received.

Syntax

To set information:

efmoam disable

To delete information:

no efmoam disable

Input mode

`(config)`

Parameters

None

Default behavior

The IEEE 802.3ah/OAM functionality operates.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

efmoam udld-detection-count

Sets the number of OAMPDU response timeouts that must occur to recognize a failure. (The OAMPDU is a monitoring packet of the IEEE 802.3ah/UDLD functionality.)

Syntax

To set or change information:

efmoam udld-detection-count <*count*>

To delete information:

no efmoam udld-detection-count

Input mode

```
(config)
```

Parameters

<*count*>

Specifies the number of OAMPDU response timeouts that must occur to determine that a line failure has occurred when timeouts occur repeatedly. When the occurrence reaches the specified number of times, the applicable port is deactivated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   3 to 300

Default behavior

30 is used as the number of times for determining a line failure.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a value smaller than the initial value is set, a unidirectional link failure might be falsely detected.

Related commands

None

Chapter

21. Storm Control

storm-control (global)
storm-control (interface)

storm-control (global)

Sets the type of frames subject to the storm control functionality.

Syntax

To set information:

no storm-control broadcast

no storm-control multicast

no storm-control unicast

To delete information:

storm-control broadcast

storm-control multicast

storm-control unicast

Input mode

`(config)`

Parameters

broadcast

Specifies that broadcast frames are not subject to storm control.

multicast

Specifies that multicast frames are not subject to storm control.

unicast

Specifies that unicast frames are not subject to storm control.

Default behavior

Broadcast, multicast, and unicast frames are all subject to the storm control functionality.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If broadcast, multicast, and unicast frames are all set as not subject to storm control, the storm control functionality does not operate.
2. To use the storm control functionality, you need to specify `upc-in-and-storm-control` using the `upc-storm-control mode` command beforehand.

Related commands

storm-control

upc-storm-control mode

storm-control (interface)

Configures the storm control functionality. This functionality sets the threshold of frames to be flooded and received by a Switch. When a broadcast storm or another problem occurs, the flooded frames exceeding the threshold are discarded. As a result, network load and Switch load decrease. When the received frame rate exceeds the threshold and the Switch detects a storm, the Switch can deactivate the port, issue an SNMP trap, and display a log message. After detecting the storm, the Switch detects recovery from the storm when the received frame rate falls below the threshold, and can issue an SNMP trap and display a log message.

Syntax

To set or change information:

storm-control level { <*rate*> | bps {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G }}

To set information:

storm-control action inactivate

storm-control action trap

storm-control action log

To delete information:

no storm-control level

no storm-control action inactivate

no storm-control action trap

no storm-control action log

Input mode

(config-if)

Parameters

level { <*rate*> | bps {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G }}

Specifies the threshold value for receive bandwidth for storm control. Frames exceeding the threshold are discarded. If 0 is set, all applicable frames are discarded.

<*rate*>

Specifies the threshold rate as a percentage of the line speed.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   0 to 100

bps {<*kbit/s*> | <*Mbit/s*>M | <*Gbit/s*>G }

Specifies the threshold bandwidth.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   The following table lists the specifiable values.

Table 21-1: Specifiable values for the storm control threshold

Setting range		Increment
In Gbit/s	1 G to 10 G	1 G#1
In Mbit/s	1 M to 10000 M	1 M#1
In kbit/s	1000 to 10000000	100 k#2
	128 to 960	64 k#3

#1: 1 G = 1000000 k. 1 M = 1000 k.

#2: When setting a value of 1000 kbit/s or more, specify the value in 100 kbit/s increments (1000, 1100, 1200...10000000).

#3: When setting a value less than 1000 kbit/s, specify the value in 64 kbit/s increments (128, 192, 256...960).

action inactivate

Deactivates the port when a storm is detected.

1. Default value when this parameter is omitted:

   If a storm is detected, only the frames exceeding the threshold are discarded. The port status does not change.

action trap

Issues an SNMP trap when a storm or the end of a storm is detected.

1. Default value when this parameter is omitted:

   If a storm is detected, no SNMP traps are issued.

action log

Outputs a log message when a storm is detected and when a storm ends.

1. Default value when this parameter is omitted:

   No log message is output when a storm is detected.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Storms are controlled by controlling the bandwidth used by the applicable frames. The number of frames is irrelevant.
2. When the received frame rates exceeds the threshold, control frames are also discarded. To prevent necessary control frames from being discarded, do not specify too small a value.
3. Storm control bandwidth limiting (`storm-control action`) occurs if a storm is detected (when the bandwidth used by received frames exceeds the bandwidth `storm-control level` threshold set for the receiving interface). After the detection of a storm, recovery from the storm is detected when the bandwidth used by received frames falls below the threshold. If a

threshold is not set, the `storm-control action` is not performed.

4. When `storm-control action inactivate` is set, if a storm has been detected and the port is deactivated, use the `activate` operation command to activate the port. If a storm is detected and a port is deactivated, no frames are received. In this state, the end of the storm cannot be detected.
5. When using SNMP traps, you must use the `snmp-server host` command to set the destination for the traps.
6. When the threshold is specified as a percentage of the line speed, the line speed is the maximum speed that can be used on the interface (1 Gbit/s for a 1-Gigabit Ethernet interface, and 10 Gbit/s for a 10-Gigabit Ethernet interface). If, due to auto-negotiation or a configuration setting, the switch interface is operating at a lower speed than its maximum speed, the storm control threshold is still the set percentage of the maximum speed.
7. To use the storm control functionality, you need to specify `upc-in-and-storm-control` using the `upc-storm-control mode` command beforehand.
8. When you set `storm-control action` for any link aggregation ports, the same setting must be specified for all ports used in the same link aggregation.
9. When `storm-control action inactivate` is set for link aggregation ports, if a storm is detected, all ports in the link aggregation are deactivated.
10. If 0 is set for the threshold receiver bandwidth value for storm control, `storm-control action` cannot be set.

Related commands

snmp-server host

storm-control (global)

upc-storm-control mode

Chapter

22. L2 Loop Detection

loop-detection
loop-detection auto-restore-time
loop-detection enable
loop-detection hold-time
loop-detection interval-time
loop-detection threshold

loop-detection

Sets the port type for the L2 loop detection functionality.

Syntax

To set or change information:

loop-detection {send-inact-port | send-port | uplink-port | exception-port}

To delete information:

no loop-detection

Input mode

`(config-if)`

Parameters

{send-inact-port | send-port | uplink-port | exception-port}

send-inact-port

Sets a port as a detecting and blocking port. When an L2 loop detection frame is sent and an L2 loop detection frame sent from the local switch is received, log data is output and the port is deactivated.

send-port

Sets a port as a detecting and sending port. When an L2 loop detection frame is sent and an L2 loop detection frame sent from the local switch is received, log data is output.

uplink-port

Sets a port as an uplink port. No L2 loop detection frames are sent. When an L2 loop detection frame from the local switch is received, log data is output to the frame source. If the port type of the frame source is a detecting and blocking port, the frame source is deactivated.

exception-port

Sets a port as port not subject to L2 loop detection. When an L2 loop detection frame is received, no operation is performed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `send-inact-port`, `send-port`, `uplink-port`, or `exception-port`

Default behavior

The port operates as a detecting port. If an L2 loop detection frame is not sent and an L2 loop detection frame sent from the local switch is detected, log data is output.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The following information is cleared when the port type is changed:

- The number of L2 loop detection frames received until the port is deactivated
- Time before automatic-restoration is performed

2. Even if the port type is changed, the statistics for sending and receiving L2 loop detection frames for each port are not cleared.

Related commands

loop-detection enable

loop-detection auto-restore-time

Sets the time (in seconds) until a deactivated port is activated automatically.

Syntax

To set or change information:

loop-detection auto-restore-time <*seconds*>

To delete information:

no loop-detection auto-restore-time

Input mode

(config)

Parameters

<*seconds*>

Sets the time (in seconds) until a deactivated port is activated automatically.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   60 to 86400

Default behavior

A deactivated port is not reactivated automatically.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command has been set and the parameter is changed, if time remains until the port is activated automatically, the change becomes effective only after the remaining time has been cleared.

Related commands

loop-detection enable

loop-detection enable

Enables the L2 loop detection functionality.

Syntax

To set or change information:

loop-detection enable id <*loop detection id*>

To delete information:

no loop-detection enable

Input mode

```
(config)
```

Parameters

id <*loop detection id*>

Sets the ID for L2 loop detection functionality. When L2 loop detection functionality is used on multiple Switches on a network, specify a unique loop detection ID for each Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 64

Default behavior

The L2 loop detection 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

loop-detection hold-time

Specifies the time (in seconds) that the number of received L2 loop detection frames is held before a port is changed to the inactive status. After an L2 loop detection frame is received, if the L2 loop detection hold time elapses without another L2 loop detection frame being received, the L2 loop detection frame count associated with the port is cleared.

Syntax

To set or change information:

loop-detection hold-time <*seconds*>

To delete information:

no loop-detection hold-time

Input mode

```
(config)
```

Parameters

<*seconds*>

Specifies the time (in seconds) that the number of received L2 loop detection frames is held before a port is changed to the inactive status.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 86400

Default behavior

Monitors (holds) the number of L2 loop detection frames received during the hold-time interval before a port is deactivated.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the parameter is changed after setting this command, then (if the hold time has not expired) the hold time is reset and the new value becomes effective.

Related commands

loop-detection enable

loop-detection interval-time

Sets the interval for sending L2 loop detection frames.

Syntax

To set or change information:

loop-detection interval-time <*seconds*>

To delete information:

no loop-detection interval-time

Input mode

(config)

Parameters

<*seconds*>

Specifies the interval (in seconds) for sending L2 loop detection frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600

Default behavior

The interval for sending L2 loop detection frames is 10 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

loop-detection enable

loop-detection threshold

Sets the number of received L2 loop detection frames before a port is deactivated.

Syntax

To set or change information:

loop-detection threshold <*count*>

To delete information:

no loop-detection threshold

Input mode

```
(config)
```

Parameters

<*count*>

Specifies the number of L2 loop detection frames that must be received before a port is deactivated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10000

Default behavior

The number of L2 loop detection frames that must be received before a port is deactivated is 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the parameter is changed after setting this command, then any received L2 loop detection frame count is cleared before setting the new parameter value.

Related commands

loop-detection enable

Chapter 23. CFM

domain name

Sets the name used for a domain.

Syntax

To set or change information:

domain name {no-present | str <*strings*> | dns <*name*> | mac <*mac*> <*id*>}

To delete information:

no domain name

Input mode

`(config-ether-cfm)`

Parameters

{no-present | str <*strings*> | 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 <*strings*>

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 <*strings*>, 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, however, that a multicast MAC address (address whose first-byte lower bit is set to 1) cannot be set.

   For <*id*>, specify a value from 0 to 65535.

Default behavior

`no-present` is set.

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` <*strings*> parameter in the `ma name` command, the first character of the specified parameter is added to CCM.

Related commands

ethernet cfm domain

ethernet cfm 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:

ethernet cfm cc level <*level*> ma <*no.*> alarm-priority <*priority*>

To delete information:

no ethernet cfm cc level <*level*> ma <*no.*> alarm-priority

Input mode

`(config)`

Parameters

level <*level*>

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*>

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<*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 23-1: Failure descriptions corresponding to the setting values

Value set	Failure type	Display in a command	Failure description
0	none	--	No failure was detected.
1	DefRDICCM	RDI	A CCM with the failure flag on was received.

Value set	Failure type	Display in a command	Failure description
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 has occurred, or a CCM with an abnormal sending interval was received.
5	DefXconCCM	OtherCCM	A CCM with a different MA was received.

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

ethernet cfm cc enable

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm 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:

ethernet cfm cc level <*level*> ma <*no.*> alarm-reset-time <*time*>

To delete information:

no ethernet cfm cc level <*level*> ma <*no.*> alarm-reset-time

Input mode

`(config)`

Parameters

level <*level*>

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*>

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<*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

ethernet cfm cc enable

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm 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:

ethernet cfm cc level <*level*> ma <*no.*> alarm-start-time <*time*>

To delete information:

no ethernet cfm cc level <*level*> ma <*no.*> alarm-start-time

Input mode

`(config)`

Parameters

level <*level*>

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*>

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<*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

ethernet cfm cc enable

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc enable

Sets in a domain an MA in which the CC functionality is used.

If the `ethernet cfm mep` command has already been set, sending from the applicable port to CCM starts.

Syntax

To set information:

ethernet cfm cc level <*level*> ma <*no.*> enable

To delete information:

no ethernet cfm cc level <*level*> ma <*no.*> enable

Input mode

`(config)`

Parameters

level <*level*>

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*>

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

Monitoring by CC is 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 domain

ma name

ma vlan-group

ethernet cfm cc interval

Sets the CCM transmission interval for a target MA.

Syntax

To set or change information:

ethernet cfm cc level <*level*> ma <*no.*> interval {1s | 10s | 1min | 10min}

To delete information:

no ethernet cfm cc level <*level*> ma <*no.*> interval

Input mode

`(config)`

Parameters

level <*level*>

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*>

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

{1s | 10s | 1min | 10min}

Sets the interval for sending CCMs.

1s

Sets the interval for sending CCMs to 1 seconds.

10s

Sets the interval for sending CCMs to 10 seconds.

1min

Sets the interval for sending CCMs to 1 minutes.

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:

`1s`, `10s`, `1min`, or `10min`

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

ethernet cfm cc enable

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm domain

Sets a domain. Executing this command switches to `config-ether-cfm` mode in which the domain name and MA can be set.

Syntax

To set information:

ethernet cfm domain level <*level*> [direction-up]

To delete information:

no ethernet cfm domain level <*level*>

Input mode

`(config)`

Parameters

level <*level*>

Specifies the domain level.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

direction-up

When up/down is not explicitly set by using the `ethernet cfm mep` command, you can set this parameter to have the Switch operate in Up MEP mode.

1. Default value when this parameter is omitted:

   The Switch operates in Down MEP mode.

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. If any of the following commands references a domain set by using this command, this command cannot be deleted:
   - ethernet cfm cc enable
   - ethernet cfm mep
   - ethernet cfm mip

Related commands

domain name

ethernet cfm cc enable

ma name

ma vlan-group

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)

When `no ethernet cfm enable` is set, CFM PDU transmission processing on the applicable port or the applicable port channel stops.

Syntax

To set information:

no ethernet cfm enable

To delete information:

ethernet cfm enable

Input mode

`(config-if)`

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 mep

Sets an MEP used by the CFM functionality.

Syntax

To set information:

ethernet cfm mep level <*level*> ma <*no.*> mep-id <*mepid*> [{down | up}]

To delete information:

no ethernet cfm mep level <*level*> ma <*no.*> mep-id <*mepid*>

Input mode

`(config-if)`

Parameters

level <*level*>

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <*no.*>

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

mep-id <*mepid*>

Sets the MEP ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8191

3. Note on using this parameter:

   Set a value unique within the MA.

{down | up}

Specifies the direction of a domain.

down

Sets the MEP as Down MEP so that the line side will be maintained.

up

Sets the MEP as Up MEP so that the relay side (toward the switch) will be maintained.

1. Default value when this parameter is omitted:

   When `direction-up` has been set by using the `ethernet cfm domain` command, Up MEP is used. If it has not been set, Down MEP is used.

2. Range of values:

   `down` or `up`

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 mip` command is set on the same interface, a domain level equal to or higher than the `ethernet cfm mip` command cannot be specified.
2. 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 mip

ethernet cfm mip

Sets an MIP used by the CFM functionality.

Syntax

To set information:

ethernet cfm mip level <*level*>

To delete information:

no ethernet cfm mip level <*level*>

Input mode

`(config-if)`

Parameters

level <*level*>

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

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 is set on the same interface, a domain level equal to or lower than the `ethernet cfm mep` command cannot be specified.
2. 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 mep

ma name

Sets the name of an MA to be used in the applicable domain.

Syntax

To set or change information:

ma <*no.*> name {str <*strings*> | vlan <*vlan id*>}

To delete information:

no ma <*no.*> name

Input mode

`(config-ether-cfm)`

Parameters

<*no.*>

Specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

{str <*strings*> | vlan <*vlan id*>}

Specifies the name of an MA by using a character string or a VLAN ID.

str <*strings*>

A character string specified for <*strings*> 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 <*strings*>, 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*>.

3. Note on using this parameter:

   - 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 <*strings*>, the 44th and subsequent characters are not used in the Short MA Name field in the CCM.

   - <*strings*> or <*vlan id*> that has already been set in the same domain cannot be specified.

Default behavior

<*no.*> of the `ma vlan-group` command is used for a name of an MA.

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 domain

ma vlan-group

Sets the VLAN belonging to the MA used in a domain.

Syntax

To set or change information:

ma <*no.*> vlan-group <*vlan id list*> [primary-vlan <*vlan id*>]

To delete information:

no ma <*no.*> vlan-group

Input mode

`(config-ether-cfm)`

Parameters

<*no.*>

Specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<*vlan id list*>

Specifies the VLANs to be used in the applicable MA.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

primary-vlan <*vlan id*>

Specifies the primary VLAN to be used when CFM PDUs are sent in the applicable MA.

1. Default value when this parameter is omitted:

   From the VLAN list specified by using `vlan-group` <*vlan id list*>, a lower-numbered VLAN is used as the primary VLAN.

2. Range of values:

   1 to 4095

3. Note on using this parameter:

   Specify the VLAN IDs specified by using `vlan-group` <*vlan id list*>.

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

ethernet cfm domain

Chapter 24. SNMP

hostname
rmon alarm
rmon collection history
rmon event
snmp-server community
snmp-server contact
snmp-server engineID local
snmp-server group
snmp-server host
snmp-server informs
snmp-server location
snmp-server traps
snmp-server user
snmp-server view
snmp trap link-status

hostname

Sets the identification name of a Switch.

Syntax

To set or change information:

hostname <*name*>

To delete information:

no hostname

Input mode

(config)

Parameters

<*name*>

The identification name of a Switch. Set a name that is unique in the network that will be used. This information can be referenced by using the name set in [sysName] in the system group for enquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the Set operation of SNMP. If this name is changed by the Set operation of SNMP, the name is applied to the configuration. This parameter is equivalent to sysName defined in RFC 1213.

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 60 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

No identification name is initially set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about name, contact, and location from the SNMP manager, you must use the snmp-server community command to register the SNMP manager.

Related commands

snmp-server community

ip domain lookup

rmon alarm

Sets the control information for the RMON (RFC 1757) alarm group. This command can configure a maximum of 128 entries.

Syntax

To set or change information:

rmon alarm <*number*> <*variable*> <*interval*> {delta | absolute} rising-threshold <*value*> rising-event-index <*event no.*> falling-threshold <*value*> falling-event-index <*event no.*> [owner string] [startup_alarm { rising_falling | rising | falling }]

To delete information:

no rmon alarm <*number*>

Input mode

`(config)`

Parameters

<*number*>

Specifies the information identification number for the RMON alarm group control information. This parameter is equivalent to `alarmIndex` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

<*variable*>

Specifies the object identifier for the MIB used for checking the threshold. This parameter is equivalent to `alarmVariable` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a MIB object identifier (in dot format) in double quotation marks. Only object identifiers that can be specified in no more than 63 characters are valid. Specify the Integer, TimeTicks, Counter, or Gauge type of the object identifier. If an input character string does not include special characters other than alphanumeric characters and periods, you do not have to enclose the character string in double quotation marks.

<*interval*>

Specifies the time interval (in seconds) for checking the threshold. This parameter is equivalent to `alarmInterval` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4294967295

{ delta | absolute }

Specifies the method for checking the threshold. If `delta` is specified, the difference between

the current value and the value of the last sampling is compared with the threshold. If `absolute` is specified, the current value is compared directly with the threshold. This parameter is equivalent to `alarmSampleType` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `delta` or `absolute`

rising-threshold <*value*>

Specifies the upper threshold. This parameter is equivalent to `alarmRisingThreshold` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   -2147483648 to 2147483647

rising-event-index <*event no.*>

Specifies the identification number of the method for generating an event if the upper threshold is exceeded. The method for generating an event is the information identification number for the control information specified by using the `event` configuration command. This parameter is equivalent to `alarmRisigEventIndex` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An information identification number from 1 to 65535 for the control information specified by using the `event` configuration command for <*event no.*>

falling-threshold <*value*>

Specifies the lower threshold value. This parameter is equivalent to `alarmFallingThreshold` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   -2147483648 to 2147483647

falling-event-index <*event no.*>

Specifies the identification number of the method for generating an event if the lower threshold is exceeded. The method for generating an event is the information identification number for the control information specified by using the `event` configuration command. This parameter is equivalent to `alarmFallingEventIndex` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An information identification number from 1 to 65535 for the control information specified by using the `event` configuration command for <*event no.*>

owner <*string*>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter is equivalent to `alarmOwner` defined in RFC 1757.

1. Default value when this parameter is omitted:

   NULL

2. Range of values:

   Enclose a character string of no more than 24 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*.

startup_alarm { rising_falling | rising | falling }

Specifies the timing for checking the threshold in the first sampling. If `rising` is specified, an alarm is generated when the upper threshold is exceeded in the first sampling. If `falling` is specified, an alarm is generated when a value drops below the lower threshold in the first sampling. If `rising_falling` is specified, an alarm is generated when the upper or lower threshold is crossed in the first sampling. This parameter is equivalent to `alarmstartUpAlarm` defined in RFC 1757.

1. Default value when this parameter is omitted:

   rising_falling

2. Range of values:

   `rising`, `falling`, or `rising_falling`

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To access an alarm group from the SNMP manager, you must register the SNMP manager by using the `snmp-server community` command.
2. As the value for `rising-event-index` or `falling-event-index` of an alarm group, set the information identification number for an event group that has been set in the switch configuration.
3. A maximum of 128 entries can be set for the alarm groups set in the configuration and set from the SNMP manager by using the `Set` operation of SNMP. When the maximum number of entries have been set, even if an alarm group is set in the configuration, the added alarm group will not work. Delete unnecessary alarm settings, and then reconfigure the alarm settings.
4. If the `Set` operation is performed from the SNMP manager for RMON alarmTable, the result of the operation will not be applied to the configuration.
5. Some alarms might not work if they cannot collect MIB information, such as when there are too many alarm configurations or when the value set for the interval is 60 seconds or less. In such a case, the MIB value for alarmStatus is `invalid(4)`. If this happens, change the interval value to 60 seconds or larger, or delete unnecessary alarm settings.

6. If the set interval value is too large, `valid(1)` is returned for the time being until alarmStatus changes from `valid(1)` to `invalid(4)` (as a guide, it takes time of about half of the interval value).

Related commands

snmp-server host

rmon event

rmon collection history

Configures the control information for the RMON (RFC 1757) Ethernet statistics history.

Syntax

To set or change information:

rmon collection history controlEntry <*integer*> [owner <*owner name*>] [buckets <*bucket number*>] [interval <*seconds*>]

To delete information:

no rmon collection history controlEntry <*integer*>

Input mode

`(config-if)`

Parameters

<*integer*>

Specifies the information identification number for the statistics history control information. This parameter is equivalent to `historyControlIndex` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

owner <*owner name*>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter is equivalent to `historyControlOwner` defined in RFC 1757.

1. Default value when this parameter is omitted:

   Blank

2. Range of values:

   Enclose a character string of no more than 24 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*.

buckets <*bucket number*>

Specifies the number of history entries in which statistics information can be stored. This parameter is equivalent to `historyControlBucketsRequested` defined in RFC 1757.

1. Default value when this parameter is omitted:

   50

2. Range of values:

   1 to 65535

   Note: If a value from 51 to 65535 is specified for <*bucket number*>, operation is the same as if 50 had been specified.

interval <*seconds*>

Specifies the time interval (in seconds) for collecting statistics information. This parameter is equivalent to `historyControlInterval` defined in RFC 1757.

1. Default value when this parameter is omitted:

   1800

2. Range of values:

   1 to 3600

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To access an Ethernet history group from the SNMP manager, you must register the SNMP manager by using the `snmp-server community` command.
2. A maximum of 32 entries can be set for the history groups set in the configuration and set from the SNMP manager by using the `Set` operation of SNMP. When the maximum number of entries have been set, even if a history group is set in the configuration, the added history group will not work. Delete unnecessary history settings, and then reconfigure the history settings.
3. If the `Set` operation is performed from the SNMP manager for RMON historyControlTable, the result of the operation will not be applied to the configuration.
4. If the NIF for the interface that has been set in RMON history configuration is deactivated, etherHistory information cannot be collected after the NIF that is deactivated. Therefore, `invalid(4)` is returned for historyControlStatus. If a long interval value is set, it takes time for historyControlStatus to change from `valid(1)` to `invalid(4)` (as a guide, it takes time of about half of the interval value).

Related commands

interface

snmp-server community

rmon event

Sets the control information for an RMON (RFC 1757) event group. This command can configure a maximum of 16 entries.

Syntax

To set or change information:

rmon event <*event no.*> [log] [trap <*community*>] [description <*string*>] [owner <*string*>]

To delete information:

no rmon event <*event no.*>

Input mode

`(config)`

Parameters

<*event no.*>

Specifies the information identification number for the control information for an RMON event group. This parameter is equivalent to `eventIndex` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

log

This parameter specifies the method for generating an alarm (event) and generates an alarm log. This parameter is equivalent to `eventType` defined in RFC 1757.

1. Default value when this parameter is omitted:

   An alarm log is not generated.

2. Range of values:

   None

trap <*community*>

This parameter specifies the method for generating an alarm (event) and sends an SNMP trap or inform to the community specified for <*community*>. This parameter is equivalent to `eventType` defined in RFC 1757.

1. Default value when this parameter is omitted:

   No traps or informs are issued.

2. Range of values:

   Sets `trap` and the community name.

   For <*community*>, enclose a character string consisting of no more than 60 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*.

description <*string*>

Uses a character string to specify the description of an event. Use this parameter as a note regarding the event. This parameter is equivalent to `eventDescription` defined in RFC 1757.

1. Default value when this parameter is omitted:

   Blank

2. Range of values:

   Enclose a character string of no more than 79 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*.

owner <*string*>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter is equivalent to `eventOwner` defined in RFC 1757.

1. Default value when this parameter is omitted:

   Blank

2. Range of values:

   Enclose a character string of no more than 24 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

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When an event group is accessed from the SNMP manager and traps or informs are sent to the SNMP manager, you must register the SNMP manager by using the `snmp-server community` and `snmp-server host` commands.
2. To send traps or informs to the SNMP manager, specify the IP address of the destination SNMP manager and `rmon` by using the `snmp-server host` command.
3. A trap or an inform is sent only if the community name used when the SNMP manager is registered matches the community name of the event group.
4. As the value for `rising-event-index` or `falling-event-index` of an alarm group, set the information identification number that has been set for the corresponding event group. If the values are different, no event is executed when an alarm is generated.
5. A maximum of 16 entries can be set for the event groups set in the configuration and set from the SNMP manager by using the `Set` operation of SNMP. When the maximum number of entries have been set, even if an event group is set in the configuration, the added event group will not work. Delete unnecessary event settings, and then reconfigure the event settings.
6. If the `Set` operation is performed from the SNMP manager for RMON eventTable, the result

of the operation will not be applied to the configuration.

Related commands

snmp-server host

rmon alarm

snmp-server community

Sets the access list for the SNMP community. A maximum of 50 addresses can be registered by this command.

Syntax

To set or change information:

snmp-server community <*community*> [{ ro | rw }] [{<*access list number*> | <*access list name*>}] [vrf <*vrf id*>]

To delete information:

no snmp-server community <*community*> [vrf <*vrf id*>]

Input mode

`(config)`

Parameters

<*community*>

Sets the community name for the SNMP manager.

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 60 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*.

{ ro | rw }

Sets the MIB operating mode for the manager that has the specified IP address belonging to the community with the specified community name. If `ro` is specified, `Get Request` and `GetNext Request` are permitted. If `rw` is set, `Get Request`, `GetNext Request`, and `Set Request` are permitted.

1. Default value when this parameter is omitted:

   ro

2. Range of values:

   `ro` or `rw`

{<*access list number*> | <*access list name*>}

Specifies the number or name of the access list in which the permissions for this community are set. If the specified {<*access list number*> | <*access list name*>} has not been set, all accesses are permitted.

One access list is permitted for one community.

1. Default value when this parameter is omitted:

   All accesses are permitted.

2. Range of values:

   For <*access list number*>, specify values from 1 to 99, or from 1300 to 1999 (in

decimal).

For <*access list name*>, specify a name that is no more than 31 characters.

For details, see *Specifiable values for parameters*.

vrf <*vrf id*> [OP-NPAR]

Permits accesses from the VRF specified in <*vrf id*>.

1. Default value when this parameter is omitted:

   Accesses from global networks are permitted.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   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

access-list

snmp-server contact

Sets the contact information of the Switch.

Syntax

To set or change information:

snmp-server contact <*contact*>

To delete information:

no snmp-server contact

Input mode

(config)

Parameters

<*contact*>

Sets the contact information for the Switch used when a failure occurs on the Switch. This information can be referenced by using the name set in [sysContact] of the system group for inquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the Set operation of SNMP. If this name is changed by the Set operation of SNMP, the name is applied to the configuration. This parameter is equivalent to sysContact defined in RFC 1213.

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 60 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 initial value is null.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about name, contact, and location from the SNMP manager, you must use the snmp-server community command to register the SNMP manager.

Related commands

None

snmp-server engineID local

Sets SNMP engine ID information.

Syntax

To set or change information:

snmp-server engineID local <*engineid string*>

To delete information:

no snmp-server engineID local

Input mode

(config)

Parameters

<*engineid string*>

Sets an SNMP engine ID.

The SNMP engine ID value set for a Switch is as follows:

1st to 4th octets: A value obtained by the OR bit of an enterprise code and 0x80000000

5th octet: Fixed value of 4

6th to 32nd octets: Setting value for <*engineid string*>

Use the snmp operation command to check the SNMP engine ID to be set for a Switch. An example is as follows.

```
> snmp get snmpEngineID.0
Name: snmpEngineID.0
Value:80 00 FF FF 04 73 6E 6D 70 5F 54 6F 6B 79 6F 31
```

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 27 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 SNMP engine ID value set for a Switch is as follows:

1st to 4th octets: A value obtained by the OR bit of an enterprise code and 0x80000000

5th octet: Fixed value of 128

6th to 9th octets: A random number

10th to 13th octets: Universal timer value when the ID is automatically generated

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If many users (a maximum of 50 users) are set by using the `snmp-server user` command, setting, changing, or deleting the `snmp-server engineID local` command takes a maximum of 20 seconds.

Related commands

snmp-server view

snmp-server user

snmp-server group

snmp-server host

snmp-server group

Sets SNMP security group information. Security level information and access control information consisting of the SNMP view information set by the `snmp-server view` command are grouped. A maximum of 50 group names can be set by this command.

Syntax

To set or change information:

snmp-server group <*group name*> v3 {noauth | auth | priv} [read <*view name*>] [write <*view name*>] [notify <*view name*>]

To delete information:

no snmp-server group <*group name*> v3 { noauth | auth | priv }

Input mode

`(config)`

Parameters

<*group name*>

Configures an SNMP security group name.

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 32 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*.

{ noauth | auth | priv }

Sets the security level of access control. When an SNMP packet is received, processing checks whether the received packet matches the security level set by this parameter. When an SNMP packet is sent, the SNMP packet is generated with the security level set by this parameter.

`noauth`: Authentication and encryption are not required.

`auth`: Authentication is required, and encryption is not required.

`priv`: Authentication and encryption are both required.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `noauth`, `auth`, or `priv`

read <*view name*>

Sets the read view name for access control. When an SNMP packet with any of the following PDU types is received, if the read view name specified for <*view name*> exists in the SNMP MIB view information, the MIB view is checked:

- GetRequest-PDU

- GetNextRequest-PDU

- GetBulkRequest-PDU

1. Default value when this parameter is omitted:

   The read access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 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*.

write <*view name*>

Sets the write view name of access control. When an SNMP packet with the SetRequest-PDU PDU type is received, if the write view name specified for <*view name*> exists in the SNMP MIB view information, the MIB view is checked.

1. Default value when this parameter is omitted:

   The write access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 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*.

notify <*view name*>

Sets the notify view name of access control. When a trap (an SNMP packet with the SNMPv2-Trap-PDU PDU type) is sent, if the notify view name specified for <*view name*> exists in the SNMP MIB view information, the MIB view is checked.

1. Default value when this parameter is omitted:

   The notify access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 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

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a MIB view name that has not been set by the `snmp-server view` command is set for the read view name, write view name, or notify view name of this command, the view name

information set by this command is invalid.

Related commands

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server host

snmp-server host

Registers the network management switch (SNMP manager) to which traps or informs are sent. This command can configure a maximum of 50 entries.

Syntax

To set or change information:

snmp-server host <*manager address*> [vrf <*vrf id*>] { traps | informs } <*string*> [version { 1 | 2c | 3 { noauth | auth | priv } }] [snmp] [{ospf_state | ospf_state_private }] [{ ospf_error | ospf_error_private }] [bgp] [vrrp] [rmon] [oadp] [air-fan] [power] [login] [memory] [system-msg] [standby_system] [temperature] [gsrp] [axrp] [frame_error_snd] [frame_error_rcv] [storm-control] [efmoam] [loop-detection] [cfm] [power-control] [static-route] [policy-base] [track-object]

To delete information:

no snmp-server host <*manager address*> [vrf <*vrf id*>]

Input mode

`(config)`

Parameters

<*manager address*>

Sets the IP address of the SNMP manager.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <*manager address*>, specify an IPv4 address (in dot notation) or an IPv6 address (in colon notation).

vrf <*vrf id*> [OP-NPAR]

Issues a trap or an inform to the VRF specified for <*vrf id*> in the `vrf definition` command.

1. Default value when this parameter is omitted:

   A trap or an inform is issued to global networks.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

{traps | informs}

Sets the type of event notification that will be sent to the SNMP manager.

- If `traps` is specified, traps will be issued. The SNMP manager does not send a response.
- If `informs` is specified, informs will be issued. Because an inform requests the SNMP manager to send a response, the SNMP agent monitors for a response. If no response is returned, the inform is resent. This parameter can be used only in version SNMPv2C.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Specify either `traps` or `informs`.

<*string*>

For SNMPv1 and SNMPv2C, this parameter sets the name of the community for the SNMP manager. For SNMPv3, this parameter sets the security user name.

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 60 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*.

version { 1 | 2c | 3 { noauth | auth | priv }}

Specifies the sending version of the manager that has the specified IP address belonging to the community with the specified community name. If `1` is specified, the SNMPv1 version traps are issued. If `2c` is specified, SNMPv2C version traps or informs are issued. If `3` is specified, SNMPv3 version traps are issued.

If `3` is specified, this parameter also sets the security level for sending the traps.

- If `noauth` is specified, traps are sent without authentication and encryption required.
- If `auth` is specified, traps are sent with authentication required and without encryption required.
- If `priv` is specified, traps are sent with both authentication and encryption required.

1. Default value when this parameter is omitted:

   1

2. Range of values:

   Specify `1`, `2c`, or `3`.

   If you specify `3`, then specify `noauth`, `auth`, or `priv`.

[snmp] [{ospf_state | ospf_state_private }] [{ ospf_error | ospf_error_private }] [bgp] [vrrp] [rmon] [oadp] [air-fan] [power] [login] [memory] [system-msg] [standby_system] [temperature] [gsrp] [axrp] [frame_error_snd] [frame_error_rcv] [storm-control] [efmoam] [loop-detection] [cfm] [power-control] [static-route] [policy-base] [track-object]

By setting each parameter, you can select the traps or informs to be sent. The following table describes traps or informs that will be sent when parameters are set.

Table 24-1: Correspondence between parameters and traps or informs

Parameter	Traps and informs
snmp	coldStart
	warmStart
	linkUp
	linkDown
	authenticationFailure
ospf_state	ospfVirtNbrStateChange

Parameter	Traps and informs
	ospfNbrStateChange
	ospfVirtIfStateChange
	ospfIfStateChange
ospf_state_private	axsOspfVirtNbrStateChange
	axsOspfNbrStateChange
	axsOspfVirtIfStateChange
	axsOspfIfStateChange
ospf_error	ospfVirtIfConfigError
	ospfIfConfigError
	ospfVirtIfAuthFailure
	ospfIfAuthFailure
ospf_error_private	axsOspfVirtIfConfigError
	axsOspfIfConfigError
	axsOspfVirtIfAuthFailure
	axsOspfIfAuthFailure
bgp	bgpEstablished
	bgpBackwardTransition
vrrp	vrrpTrapNewMaster
	vrrpTrapAuthFailure
	vrrpTrapProtoError
rmon	risingAlarm
	fallingAlarm
oadp	axsOadpNeighborCachelastChangeTrap
air-fan	ax6700sAirFanStopTrap [AX6700S] ax6600sAirFanStopTrap [AX6600S] ax6300sAirFanStopTrap [AX6300S]
power	ax6700sPowerSupplyFailureTrap [AX6700S] ax6600sPowerSupplyFailureTrap [AX6600S] ax6300sPowerSupplyFailureTrap [AX6300S]
login	ax6700sLoginSuccessTrap [AX6700S] ax6600sLoginSuccessTrap [AX6600S] ax6300sLoginSuccessTrap [AX6300S]
	ax6700sLoginFailureTrap [AX6700S] ax6600sLoginFailureTrap [AX6600S] ax6300sLoginFailureTrap [AX6300S]
	ax6700sLogoutTrap [AX6700S] ax6600sLogoutTrap [AX6600S] ax6300sLogoutTrap [AX6300S]

Parameter	Traps and informs
memory	ax6700sMemoryUsageTrap [AX6700S] ax6600sMemoryUsageTrap [AX6600S] ax6300sMemoryUsageTrap [AX6300S]
system-msg	ax6700sSystemMsgTrap [AX6700S] ax6600sSystemMsgTrap [AX6600S] ax6300sSystemMsgTrap [AX6300S]
standby_system	ax6700sStandbySystemUpTrap [AX6700S] ax6700sStandbyBsuUpTrap [AX6700S] ax6700sStandbyNifUpTrap [AX6700S] ax6600sStandbySystemUpTrap [AX6600S] ax6600sStandbyNifUpTrap [AX6600S] ax6300sStandbySystemUpTrap [AX6300S]
	ax6700sStandbySystemDownTrap [AX6700S] ax6700sStandbyBsuDownTrap [AX6700S] ax6700sStandbyNifDownTrap [AX6700S] ax6600sStandbySystemDownTrap [AX6600S] ax6600sStandbyNifDownTrap [AX6600S] ax6300sStandbySystemDownTrap [AX6300S]
temperature	ax6700sTemperatureTrap [AX6700S] ax6600sTemperatureTrap [AX6600S] ax6300sTemperatureTrap [AX6300S]
gsrp	ax6700sGsrpStateTransitionTrap [AX6700S] ax6600sGsrpStateTransitionTrap [AX6600S] ax6300sGsrpStateTransitionTrap [AX6300S]
axrp	ax6700sAxrpStateTransitionTrap [AX6700S] ax6600sAxrpStateTransitionTrap [AX6600S] ax6300sAxrpStateTransitionTrap [AX6300S]
frame_error_snd	ax6700sFrameErrorSendTrap [AX6700S] ax6600sFrameErrorSendTrap [AX6600S] ax6300sFrameErrorSendTrap [AX6300S]
frame_error_rcv	ax6700sFrameErrorReceiveTrap [AX6700S] ax6600sFrameErrorReceiveTrap [AX6600S] ax6300sFrameErrorReceiveTrap [AX6300S]
storm-control	ax6700sStormDetectTrap [AX6700S] ax6600sStormDetectTrap [AX6600S] ax6300sStormDetectTrap [AX6300S]
	ax6700sStormPortInactivateTrap [AX6700S] ax6600sStormPortInactivateTrap [AX6600S] ax6300sStormPortInactivateTrap [AX6300S]
	ax6700sStormRecoverTrap [AX6700S] ax6600sStormRecoverTrap [AX6600S] ax6300sStormRecoverTrap [AX6300S]
efmoam	ax6700sEfmoamUdldPortInactivateTrap [AX6700S] ax6600sEfmoamUdldPortInactivateTrap [AX6600S] ax6300sEfmoamUdldPortInactivateTrap [AX6300S]
	ax6700sEfmoamLoopDetectPortInactivateTrap [AX6700S] ax6600sEfmoamLoopDetectPortInactivateTrap [AX6600S] ax6300sEfmoamLoopDetectPortInactivateTrap [AX6300S]

Parameter	Traps and informs
loop-detection	ax6700sL2ldLinkDown [AX6700S] ax6600sL2ldLinkDown [AX6600S] ax6300sL2ldLinkDown [AX6300S]
	ax6700sL2ldLinkUp [AX6700S] ax6600sL2ldLinkUp [AX6600S] ax6300sL2ldLinkUp [AX6300S]
	ax6700sL2ldLoopDetection [AX6700S] ax6600sL2ldLoopDetection [AX6600S] ax6300sL2ldLoopDetection [AX6300S]
cfm	dot1agCfmFaultAlarm
power-control	ax6700sPowerControlModeChangeStartTrap [AX6700S] ax6600sPowerControlModeChangeStartTrap [AX6600S]
	ax6700sPowerControlModeChangeCompleteTrap [AX6700S] ax6600sPowerControlModeChangeCompleteTrap [AX6600S]
static-route	axsStaticGatewayStateChange
	axsStaticIpv6GatewayStateChange
policy-base	axsPolicyBaseRoutingRouteChange
	axsPolicyBaseSwitchingRouteChange
track-object	axsTrackObjectStateChange

snmp

`coldStart`, `warmStart`, `linkDown`, `linkUp`, and `authenticationFailure` traps or informs are sent.

{ ospf_state | ospf_state_private }

Sends a trap or an inform for notifying a change in the OSPF status. If `ospf_state` is specified, a standard trap or inform that complies with the RFC is issued. However, if the OSPF domain is being partitioned, all domains other than the domain with the smallest domain number will issue private traps or informs. If `ospf_state_private` is specified, all OSPF domains will issue private traps or informs.

The following table lists the traps or informs to be issued.

Table 24-2: Traps and informs to be issued for each parameter (Notifying the change of the OSPF status)

Parameter	Traps and informs to be issued
ospf_state	Domain with the smallest domain number: • ospfVirtIfStateChange • ospfNbrStateChange • ospfVirtNbrStateChange • ospfIfStateChange All domains other than the domain with the smallest domain number: • axsOspfVirtIfStateChange • axsOspfNbrStateChange • axsOspfVirtNbrStateChange • axsOspfIfStateChange

Parameter	Traps and informs to be issued
ospf_state_private	All domains: • axsOspfVirtIfStateChange • axsOspfNbrStateChange • axsOspfVirtNbrStateChange • axsOspfIfStateChange

{ ospf_error | ospf_error_private }

Sends a trap or an inform for notifying reception of an OSPF error packet. If `ospf_error` is specified, a standard trap or inform that complies with the RFC is issued. However, if the OSPF domain is being partitioned, all domains other than the domain with the smallest domain number will issue private traps or informs. If `ospf_error_private` is specified, all OSPF domains will issue private traps or informs.

The following table lists the traps or informs to be issued.

Table 24-3: Traps and informs to be issued for each parameter (Notifying reception of an OSPF error packet)

Parameter	Traps and informs to be issued
ospf_error	Domain with the smallest domain number: • ospfIfConfigError • ospfVirtIfConfigError • ospfIfAuthFailure • ospfVirtIfAuthFailure All domains other than the domain with the smallest domain number: • axsOspfIfConfigError • axsOspfVirtIfConfigError • axsOspfIfAuthFailure • axsOspfVirtIfAuthFailure
ospf_error_private	All domains: • axsOspfIfConfigError • axsOspfVirtIfConfigError • axsOspfIfAuthFailure • axsOspfVirtIfAuthFailure

bgp

A trap or an inform is sent when a BGP link is established or closed.

vrrp

A trap or an inform is sent when the VRRP status is changed.

rmon

A trap or an inform is sent when the value exceeds the upper threshold or drops below the lower threshold of the `rmon` alarm.

oadp

A trap or an inform is sent when information on an OADP neighboring node is updated.

air-fan

A trap or an inform is sent when a fan stops.

power

A trap or an inform is sent when a failure occurs in a power supply unit.

login

A trap or an inform is sent when a login fails or succeeds or when a logout occurs.

memory

A trap or an inform is sent when a memory shortage occurs in the Switch.

system-msg

A trap or an inform is sent when a system message is output.

standby_system

- For AX6700S series switches:

  A trap or an inform is sent when the operating status of a standby BCU, BSU, or NIF is changed from operating status to a status other than operating status, or changed from a status other than operating status to operating status.

- For AX6600S series switches:

  A trap or an inform is sent when the operating status of a standby CSU or NIF is changed from operating status to a status other than operating status, or changed from a status other than operating status to operating status.

- For AX6300S series switches:

  A trap or an inform is sent when the operating status of a standby MSU is changed from operating status to a status other than operating status, or changed from a status other than operating status to operating status.

temperature

A trap is sent when the temperature changes.

gsrp

A trap or an inform is sent when the GSRP status is changed.

axrp

A trap or an inform is sent when the ring failure monitoring status is changed.

frame_error_snd

A trap or an inform is sent when a frame reception error occurs.

frame_error_rcv

A trap or an inform is sent when a frame sending error occurs.

storm-control

A trap or an inform is sent when a storm is detected by the storm control functionality or when a Switch recovers from a storm.

efmoam

A trap or an inform is sent when a unidirectional link failure is detected.

loop-detection

A trap or an inform is sent when an L2 loop is detected.

cfm

A trap or an inform is sent when a failure is detected by CC.

power-control [AX6700S] [AX6600S]

Sends traps or informs for the start and end of power control mode change due to power saving functionality triggered by scheduling or traffic volume.

static-route

A trap or an inform is issued when the status of a gateway that uses dynamic monitoring for static routing changes.

policy-base

A trap or an inform is sent when route information for policy-based routing is changed or the destination interface information for policy-based switching is changed.

track-object

A private MIB trap is sent when the track status of the tracking function for policy-based routing has changed.

1. Default value when this parameter is omitted:

   A trap or an inform is not issued for each parameter.

2. Range of values:

   snmp, ospf_state or ospf_state_private, ospf_error or ospf_error_private, bgp, vrrp, rmon, oadp, air-fan, power, login, memory, system-msg, standby_system, temperature, gsrp, axrp, frame_error_snd, frame_error_rcv, storm-control, efmoam, loop-detection, cfm, power-control, static-route, policy-base, track-object

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the list of supported MIBs and supported traps, see *MIB Reference For Version 11.7*.
2. When `3` has been set for the version, if a security user name that has not been set in the `snmp-server user` command is set by this command, the security user information set in this command is invalid.

Related commands

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server group

snmp-server informs

Sets the conditions for sending informs. This setting is valid for SNMP managers for which the `informs` parameter of the `snmp-server host` command is set.

Syntax

To set or change information:

snmp-server informs [retries <*retries*>] [timeout <*seconds*>] [pending <*pending*>]

To delete information:

no snmp-server informs

Input mode

`(config)`

Parameters

retries <*retries*>

Sets the maximum number of times an inform can be resent to the SNMP manager. If 0 is set, resending is not performed.

1. Default value when this parameter is omitted:

   3

2. Range of values:

   0 to 100

timeout <*seconds*>

Sets the timeout time in seconds for informs to the SNMP manager.

1. Default value when this parameter is omitted:

   30

2. Range of values:

   1 to 21474835

pending <*pending*>

Sets the maximum number of inform events that the Switch can retain at the same time. If the SNMP manager does not respond, an inform event is held. If the number of inform events retained exceeds the maximum, excess events are discarded starting from the oldest ones.

1. Default value when this parameter is omitted:

   25

2. Range of values:

   1 to 21000

Default behavior

The initial values for all parameters of this command are used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

snmp-server host

snmp-server location

Sets the name of the location where the Switch is installed.

Syntax

To set or change information:

snmp-server location <*location*>

To delete information:

no snmp-server location

Input mode

(config)

Parameters

<*location*>

Sets the name of the location where the Switch is installed. This information can be referenced by using the name set in [sysLocation] of the system group for inquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the Set operation of SNMP. If this name is changed by the Set operation of SNMP, the name is applied to the configuration. This parameter is equivalent to sysLocation defined in RFC 1213.

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 60 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 initial value is null.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about name, contact, and location from the SNMP manager, you must use the snmp-server community command to register the SNMP manager.

Related commands

None

snmp-server traps

Sets the timing for issuing a trap or an inform.

Syntax

To set or change information:

snmp-server traps [{ limited_coldstart_trap | unlimited_coldstart_trap }] [link_trap_bind_info { private | standard }] [system_msg_trap_level <*level*>] [agent-address <*agent address*>]

To delete information:

no snmp-server traps

Input mode

`(config)`

Parameters

{ limited_coldstart_trap | unlimited_coldstart_trap }

Limits the times when `coldStart Trap` is issued. The following table provides an overview of the events that cause the `coldStart Trap` set by using this parameter to be issued.

Table 24-4: Events causing coldStart Trap to be issued for each parameter

Parameter	Events
limited_coldstart_trap	• When a device starts • When a switchover has occurred
unlimited_coldstart_trap	• When a device starts • When the IP address of a VLAN is added, deleted, or changed due to a change in the configuration • When the running configuration is changed by using the `copy` command • When the time is changed by using the `set clock` command • When a switchover has occurred

1. Default value when this parameter is omitted:

   limited_coldstart_trap

2. Range of values:

   `limited_coldstart_trap` or `unlimited_coldstart_trap`

link_trap_bind_info {private | standard}

Configures the MIB to be added when a `linkDown` or `linkUp` trap is issued.

The following table describes the MIBs to be added when a `linkDown` or `linkUp` trap set by using this parameter is issued.

Table 24-5: MIBs to be added when a linkDown or linkUp trap is issued for each parameter

Parameter	MIBs to be added when a linkDown or linkUp trap is issued
private	• (Common to SNMPv1 and SNMPv2C) `ifIndex`, `ifDescr`, and `ifType`
standard	• (For SNMPv1) `ifIndex` • (For SNMPv2C) `ifIndex`, `ifAdminStatus`, and `ifOperStatus`

1. Default value when this parameter is omitted:

   standard

2. Range of values:

   `private` or `standard`

system_msg_trap_level <*level*>

Specifies the level of sending system message traps among private traps or informs (in decimal). The following table describes the overview of the system message traps to be issued for each level specified by this command.

Table 24-6: Level of system message traps and their meanings

Level	Meaning
9	Sends a system message trap for a fatal failure.
8	Sends a system message trap for a severe failure or higher failure.
7	Sends a system message trap for a software failure or higher failure.
6	Sends a system message trap for a NIF failure or higher failure.
5	Sends a system message trap for a standby BCU, standby BSU, standby CSU, or standby MSU failure, or higher failure.
4	Sends a system message trap for a network failure or higher failure.
1 to 3	Sends a system message trap for a warning level failure or higher failure.

1. Default value when this parameter is omitted:

   9

2. Range of values:

   1 to 9

   Note: If a value from `1` to `3` is specified for <*Level*>, operation is the same as if `3` had been specified.

agent-address <*agent address*>

Specifies the IPv4 address to be used for the agent address in a trap notification frame in SNMPv1 format. Because only the SNMPv1 frame format can have the agent address field in Trap-PDUs, the address set by using this command is applied to SNMPv1 traps.

Note that this parameter is applied only to the traps to be issued to global networks.

1. Default value when this parameter is omitted:

   When this parameter has not been set, if an IPv4 address has been set for interface loopback, that address is used for the agent address. If such an address has not been set, the IPv4 address for the interface that has the lowest ifIndex is used as the agent address in a trap notification frame. This interface must be a management port or VLAN interface. If no IPv4 address has been set for the Switch, `0.0.0.0` is used.

2. Range of values:

   Specify an IPv4 address from `0.0.0.0` to `255.255.255.255` for <*agent address*>.

Default behavior

The initial values for all parameters of this command are used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the list of supported MIBs and supported traps, see *MIB Reference For Version 11.7*.

Related commands

None

snmp-server user

Sets SNMP security user information. The user information created by this command is to be used in the `snmp-server group` command and the `snmp-server host` command. This command can configure a maximum of 50 entries.

This command configures the authentication protocol and the encryption protocol. You can configure the encryption protocol after the authentication protocol has been configured. The following table lists the combinations of the authentication protocols and the encryption protocols.

Table 24-7: Combination of the authentication protocol and the encryption protocol

#	Authentication protocol	Encryption protocol
1	None	None
2	MD5 or SHA	None
3	MD5 or SHA	DES

Syntax

To set or change information:

snmp-server user <*user name*> <*group name*> v3 [auth { md5 | sha } <*authentication password*> [priv des <*privacy password*>]] [vrf <*vrf id*>]

To delete information:

no snmp-server user <*user name*>

Input mode

`(config)`

Parameters

<*user name*>

Configures an SNMP security user name.

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 32 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*.

<*group name*>

Sets the name of the SNMP security group to which the SNMP security user belongs.

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 32 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*.

v3 [auth { md5 | sha } <*authentication password*> [priv des <*privacy password*>]]

auth { md5 | sha } <*authentication password*>

Specifies the authentication protocol and the authentication password.

`md5`: HMAC-MD5 is used for the authentication protocol.

`sha`: HMAC-SHA1 is used for the authentication protocol.

priv des <*privacy password*>

Specifies the encryption protocol and the encryption password.

1. Default value when this parameter is omitted:

   If `auth` and subsequent parameter options are omitted, an authentication protocol will not be used.

   If `priv des` and subsequent parameter options are omitted, an encryption protocol will not be used.

2. Range of values:

   `v3 auth md5` <*authentication password*>, `v3 auth sha` <*authentication password*>, `v3 auth md5` <*authentication password*> `priv des` <*privacy password*>, or `v3 auth sha` <*authentication password*> `priv des` <*privacy password*>

   For <*authentication password*> and <*privacy password*>, set a character string consisting of 8 to 32 characters, enclosed 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*.

vrf <*vrf id*> [OP-NPAR]

Permits accesses from the VRF specified in <*vrf id*>.

1. Default value when this parameter is omitted:

   Accesses from global networks are permitted.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   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

1. If a security group name that has not been set by the `snmp-server group` command is set in this command, the security group information set in this command will be invalid.

Related commands

snmp-server engineID local

snmp-server view

snmp-server group

snmp-server host

snmp-server view

Sets MIB view information. The MIB view information is used to check the object ID for Variable Bindings contained in SNMP PDUs. The MIB view consists of one subtree or multiple subtrees. A subtree is set by the combination of the object ID and view type. The MIB view created by this command is to be used in the `snmp-server group` command.

The following table lists the number of entries for each parameter that can be set in this command.

Table 24-8: Number of entries for each parameter

#	Parameter	Maximum number of entries
1	MIB view	50 entries per device
2	Subtree	30 entries for a MIB view
3		500 entries per device

Syntax

To set or change information:

snmp-server view <*view name*> <*oid tree*> { included | excluded }

To delete information:

no snmp-server view <*view name*> <*oid tree*>

Input mode

`(config)`

Parameters

<*view name*>

Sets a MIB view name.

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 32 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*.

<*oid tree*>

Sets an object ID that indicates a subtree.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an object ID in dot notation. You can use no more than 64 characters. You can also use a wildcard (`*`) for each sub-ID (numbers separated by a period).

{ included | excluded }

Sets the inclusion or exclusion of a subtree. Specify `included` to include the subtree in the MIB view. Specify `excluded` to exclude the subtree from the MIB view.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify either `included` or `excluded`.

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 you change or delete information, if a wildcard (`*`) is specified for a sub-ID for <*oid tree*>, this entry is regarded as the same as the entry for which the sub-ID of the same position is `0`. Also, if you set `0` for a sub-ID, this entry is regarded as the same as the entry for which the sub-ID of the same position is a wildcard (`*`).

   Therefore, if you change information for one entry, information of another entry is also overwritten. If you delete information for one entry, information of another entry is also deleted.

   Example:

```
(config)#  show snmp-server
snmp-server view "READ_VIEW" 1.0.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# snmp-server view "READ_VIEW" 1.*.1.1 included
(config)#  show snmp-server
snmp-server view "READ_VIEW" 1.*.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# no snmp-server view "READ_VIEW" 1.0.1.1
(config)#  show snmp-server
snmp-server view "READ_VIEW" 1.1.1.1 excluded
```

Related commands

snmp-server engineID local

snmp-server user

snmp-server group

snmp-server host

snmp trap link-status

Prevents a trap or an inform (`linkDown` and `linkUp` traps) from being sent when a link-up failure or a link-down failure occurs on a line.

Syntax

To set information:

```
no snmp trap link-status
```

To delete information:

```
snmp trap link-status
```

Input mode

```
(config-if)
```

Parameters

None

Default behavior

Sending traps or informs (`linkDown` and `linkUp` traps) is not suppressed.

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

25. Log Data Output Functionality

logging email
logging email-event-kind
logging email-from
logging email-interval
logging email-server
logging event-kind
logging facility
logging host
logging syslog-dump
logging trap

logging email

Sets the email address to which log information is output as an email. This command can configure a maximum of 64 entries.

Syntax

To set information:

logging email <*e-mail address*>

To delete information:

no logging email <*e-mail address*>

Input mode

`(config)`

Parameters

<*e-mail address*>

Specifies the destination email address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   You can use only alphanumeric characters, hyphens (-), underscores (_), periods (.), and at marks (@) with no more than 255 characters.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You must use the `logging email-server` command beforehand to set the SMTP server to which an email is sent.
2. You must configure the settings related to the DNS resolver functionality beforehand.
3. Make sure that the specified email address matches the address set for the destination SMTP server.
4. If an attempt to send an email fails, the email is discarded.
5. If an IP address is set for the loopback interface, the IP address is used as the source IP address during communication with the SMTP server.
6. When you use an at mark (`@`) in an email address, do not use it for the beginning or ending of the email address. Also, do not specify multiple at marks.

Related commands

logging email-server

hostname

ip domain name

ip name-server

ip domain lookup

logging email-event-kind

Sets the event type of log information to be output as an email. Multiple event types can be set.

Syntax

To set information:

logging email-event-kind <*event kind*>

To delete information:

no logging email-event-kind <*event kind*>

Input mode

`(config)`

Parameters

<*event kind*>

Specifies the event type of the log information to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `key`, `rsp`, `rtm`, `err`, `evt`, `mrp`, `mr6`, `aut`, `acl`, `dsn`, or `tro`.

Default behavior

`evt` or `err` is set as the event type.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The event type set by using this command is applied to all destination email addresses specified by using this command.
2. If the event type is set by using this command, the default event types (`evt` and `err`) become invalid and only the event types that have been set take effect.

Related commands

logging email

logging email-from

Sets the sender of the log information output as an email.

Syntax

To set or change information:

logging email-from <*e-mail address*>

To delete information:

no logging email-from

Input mode

(config)

Parameters

<*e-mail address*>

Specifies the source email address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   You can use only alphanumeric characters, hyphens (-), underscores (_), periods (.), and at marks (@) with no more than 255 characters.

Default behavior

The sender of the email is device-name<*nobody*>, where device-name is the name specified by the hostname command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The sender of the email set by using this command is applied to all destination email addresses specified by using this command.
2. When you use an at mark (@) in an email address, do not use it for the beginning or ending of the email address. Also, do not specify multiple at marks.

Related commands

logging email

logging email-interval

Sets the interval for sending output log information as an email.

Syntax

To set or change information:

logging email-interval <*seconds*>

To delete information:

no logging email-interval

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the interval for sending emails.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600 (seconds)

Default behavior

The interval for sending emails is set to `1`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The interval for sending emails that is set by using this command is applied to all destination email addresses specified by using this command.

Related commands

logging email

logging email-server

Sets the SMTP server information for outputting log information as an email. This command can configure a maximum of 16 entries.

Syntax

To set information:

logging email-server {<*host name*> | <*ip address*>} [port <*port number*>]

To delete information:

no logging email-server {<*host name*> | <*ip address*>}

Input mode

```
(config)
```

Parameters

{<*host name*> | <*ip address*>}

Specifies the host name or IP address of the SMTP server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*host name*>

   Specifies a host name with no more than 64 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

   <*ip address*>

   Specifies the IPv4 address in dot notation.

port <*port number*>

Specifies the SMTP server port number.

1. Default value when this parameter is omitted:

   25

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. Make sure that the specified SMTP server information (the host name or IP address, and port number) matches the one set for the destination SMTP server. If the connection to the SMTP server fails while an email is being sent, the email is discarded.

2. This functionality can use IPv4 only. Therefore, if you specify as the SMTP server the name of a host that has only an IPv6 address set by using the `ipv6 host` command, emails sent to the server will be discarded.
3. `localhost` cannot be set as a host name.
4. Host names are not case sensitive.
5. `127.*.*.*` cannot be set as an IPv4 address.
6. A class D or class E address cannot be specified as an IPv4 address.
7. If large amounts of log information are generated at one time, some of the information might be missing from the log emails.

Related commands

ip host

logging email

hostname

ip domain name

ip name-server

ip domain lookup

logging event-kind

Sets the event type of the log information to be sent to the syslog server. Multiple event types can be set.

Syntax

To set information:

logging event-kind <*event kind*>

To delete information:

no logging event-kind <*event kind*>

Input mode

`(config)`

Parameters

<*event kind*>

Specifies the event type of the log information to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `key`, `rsp`, `rtm`, `err`, `evt`, `mrp`, `mr6`, `aut`, `acl`, `dsn`, or `tro`.

Default behavior

`evt` or `err` is set as the event type.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The event type set by using this command is applied to all output destinations specified by using this command.
2. If the event type is set by using this command, the default event types (`evt` and `err`) become invalid and only the event types that have been set take effect.

Related commands

logging host

logging facility

Sets a facility to which log information is output via the syslog interface.

Syntax

To set or change information:

logging facility <*facility*>

To delete information:

no logging facility

Input mode

`(config)`

Parameters

<*facility*>

Specifies the facility for syslog.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `local0`, `local1`, `local2`, `local3`, `local4`, `local5`, `local6`, or `local7`.

Default behavior

`local0` is used as the facility.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The facility set by using this command is applied to all output destinations specified by using this command.

Related commands

logging host

logging host

Sets the output destination for log information. The command can configure up to 20 entries.

Syntax

To set information:

logging host <*host name*> [no-date-info]

logging host { <*ip address*> | <*ipv6 address*> } [vrf <*vrf id*>] [no-date-info]

To delete information:

no logging host <*host name*>

no logging host { <*ip address*> | <*ipv6 address*> } [vrf <*vrf id*>]

Input mode

`(config)`

Parameters

<*host name*>

Specifies the name of a host to which log information is to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies a host name with no more than 64 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

{ <*ip address*> | <*ipv6 address*> }

Specifies an IPv4 or IPv6 address to which log information is to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <*ip address*>

   Specifies the IPv4 address in dot notation.

   <*ipv6 address*>

   Specifies the IPv6 address in colon notation.

vrf <*vrf id*> [OP-NPAR]

Sends log information to the VRF specified for the <*vrf id*> parameter in the `vrf definition` command.

1. Default value when this parameter is omitted:

   Log information is sent to global networks.

2. Range of values:

   For <*vrf id*>, specify a VRF ID.

   For details, see *Specifiable values for parameters*.

no-date-info

Sends the information after excluding the time from log information.

If the log type is `EVT` or `ERR`, the information after excluding the time, message ID, and additional information is sent.

For details about the log information format, see *1.2.3 Format of operation logs* in the manual *Message and Log Reference For Version Ver. 11.7*.

1. Default value when this parameter is omitted:

   All log information is sent.

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. To use the syslog functionality, a syslog daemon program must be running on the destination host and the host must be configured so that it can receive the syslog information from the Switch.
2. If an IP address is set for the loopback interface, the IP address is used as the source IP address from which syslog information is sent.
3. `localhost` cannot be specified as a host name.
4. Host names are not case sensitive.
5. `127.*.*.*` cannot be set as an IPv4 address.
6. A class D or class E IPv4 address cannot be set.
7. IPv6 addresses can be global addresses or site-local addresses.
8. If a large amount of log information is generated at one time, some information might be missing from the syslog information.
9. Even if `no-date-info` is specified, time information remains in the log information saved in the device.
10. If `no-date-info` is specified, time information is excluded from the body of the message sent to the log output destination. However, because the log output functionality adds time information to the message header, the date and time when the log information was sent are displayed in the message at the log output destination.

Related commands

ip host

ipv6 host

hostname

ip domain name

ip name-server

ip domain lookup

logging syslog-dump

Configures the settings so that log data generated on a switch is not stored in the internal flash memory.

Syntax

To set information:

no logging syslog-dump

To delete information:

logging syslog-dump

Input mode

`(config)`

Parameters

None

Default behavior

Log data is stored in the internal flash memory.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Log data mentioned here includes operation logs (`/usr/var/log/system.log`) and reference logs (`/usr/var/log/error.log`).
2. We recommend that you send log data via the syslog interface because this setting does not store log data in the Switch.
3. Even if this setting has been configured, the startup log data and the log data for the cause of the startup that is output when the Switch starts is saved in the internal flash memory.
4. Executing the `clear logging` operation command accesses the internal flash memory and erases the log data.

Related commands

logging host

logging trap

Sets the level of importance for log information to be sent to the syslog server.

Syntax

To set or change information:

logging trap { <*level*> | <*keyword*> }

To delete information:

no logging trap

Input mode

`(config)`

Parameters

{ <*level*> | <*keyword*> }

Select either a level or a keyword as the priority of syslog messages.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The table below describes the priorities that can be specified. Note that if a level is specified, information is displayed with the keyword.

Table 25-1: Priorities that can be specified

Level	Keyword	Description
0	emergencies	System unavailable
1	alerts	Immediate action required
2	critical	Critical state
3	errors	Error state
4	warnings	Warning state
5	notifications	Normal but attention required
6	information	Message reporting information
7	debugging	Message displayed during debugging only

Default behavior

`information` (priority level 6) is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The priority set by using this command is applied to all output destinations set by using this command.

Related commands

logging host

Chapter

26. sFlow Statistics

sflow destination
sflow extended-information-type
sflow forward egress
sflow forward ingress
sflow max-header-size
sflow max-packet-size
sflow packet-information-type
sflow polling-interval
sflow sample
sflow source
sflow url-port-add
sflow version

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:

   1 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 { [switch] [router] [gateway] [user] [url] | none }

To delete information:

no sflow extended-information-type

Input mode

(config)

Parameters

{ [switch] [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 *30.1.3(2)(c) Extended data format* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

Multiple parameters can be specified at one time. 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.

switch

Enables the sending of switch information (such as VLAN information).

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:

   switch, router, gateway, user, url, 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 egress

Causes the send traffic of the specified port to be monitored by the sFlow statistics functionality.

Syntax

To set information:

sflow forward egress

To delete information:

no sflow forward egress

Input mode

(config-if)

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 forward ingress

Causes the received traffic of the specified port to be monitored by the sFlow statistics functionality.

Syntax

To set information:

sflow forward ingress

To delete information:

no sflow forward ingress

Input mode

(config-if)

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

If the header type is used for the basic data format (see the `sflow packet-information-type` command), sets the maximum size from the beginning of the sample packet to be copied.

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.

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.

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.

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 for the 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 *30.1.3(2)(b) Basic data format* in the manual *Configuration Guide Vol. 2 For Version 11.7*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   ip

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 Switch 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 Switch.

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 Switch. 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 PPS (number of packets per second) information from the operating status of the port for which sFlow statistics are to be enabled. The recommended value is described in *Table 26-1: Sampling interval to be used as a guideline in an operating environment* in the *Sampling interval to be used as a guideline* column for the applicable total PPS value. If you set a sampling interval that is significantly smaller than the recommended value, the load on the CPU might be excessive.

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, 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 26-2: 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 26-1: Sampling interval to be used as a guideline in an operating environment

Total PPS	Sampling interval to be used as a guideline	Example implementation to be used as a guideline
Up to 4 kpps	8	
Up to 16 kpps	32	
Up to 64 kpps	128	100-Mbit/s Ethernet x 1
Up to 256 kpps	512	
Up to 1 Mpps	2048	1-Gbit/s Ethernet x 1
Up to 4 Mpps	8192	10-Gbit/s Ethernet x 1
Up to 16 Mpps	32768	

Total PPS	Sampling interval to be used as a guideline	Example implementation to be used as a guideline
Up to 64 Mpps	131072	1-Gbit/s Ethernet x 48
Up to 256 Mpps	524288	
Up to 1 Gpps	2097152	

Table 26-2: 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 Switch 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 `egress` has been specified in the `sflow forward` command, the specifiable range of values for the sampling interval is 2 or more.

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 priority 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 priority.

Priority 1

The loopback address (when a loopback address has been set by the configuration command)

Priority 2

An IP address is automatically assigned from the IP address assigned to a Switch port.

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 a Switch port. If the specified IP address is not the one set for the Switch, sFlow packets cannot be sent.

Related commands

None

sflow url-port-add

When URL information is used in the extended data format, sets the port number used for HTTP packets to a port number other than 80.

Syntax

To set or change information:

sflow url-port-add <*url port*>

To delete information:

no sflow url-port-add

Input mode

(config)

Parameters

<*url port*>

When URL information is used in the extended data format, sets the port number used for HTTP packets to a port number other than 80.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 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 version

Sets the version of the sFlow packet to be sent.

Syntax

To set information:

sflow version <*version no.*>

To delete information:

no sflow version

Input mode

`(config)`

Parameters

<*version no.*>

Sets the version of the sFlow packet to be sent. The sFlow packet of the specified version is sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2

Default behavior

The version of the sFlow packet is 4.

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 27. 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)

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 how long the LLDP frames sent from the Switch to neighboring devices will be retained on the neighboring devices.

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 value specified by the `lldp interval-time` command as the time that a neighboring device retains the LLDP frame sent from the Switch. If the time exceeds 65535, which is the maximum value, 65535 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 time that a neighboring device retains LLDP frames sent from the Switch.

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 Switch 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 Switch.

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 Switch.

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

28. OADP

oadp cdp-listener
oadp enable
oadp hold-time
oadp ignore-vlan
oadp interval-time
oadp run

oadp cdp-listener

Specifies whether the CDP reception functionality is enabled on the Switch.

Syntax

To set information:

oadp cdp-listener

To delete information:

no oadp cdp-listener

Input mode

(config)

Parameters

None

Default behavior

The CDP reception 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

oadp enable

Enables OADP for a port or link aggregation.

Syntax

To set information:

oadp enable

To delete information:

no oadp enable

Input mode

(config-if)

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

1. Even if this command is set for a port that is a member of a link aggregation, the OADP functionality does not work. The OADP functionality works for each link aggregation.

Related commands

oadp run

oadp cdp-listener

oadp hold-time

Specifies how long the OADP frames sent from the Switch to neighboring devices will be retained on the neighboring devices.

Syntax

To set or change information:

oadp hold-time <*seconds*>

To delete information:

no oadp hold-time

Input mode

`(config)`

Parameters

<*seconds*>

Specifies how long the OADP frames sent from the Switch to neighboring devices will be retained on the neighboring devices (in seconds).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 255

Default behavior

The period of time the neighboring devices will retain the OADP frames sent from the Switch is three times the value set by the `oadp interval-time` command. If the value that is three times of the set value exceeds 255 seconds, the period of time is set to 255 seconds.

If the `oadp interval-time` command is omitted, the period of time is set to 180 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The value set by the `oadp hold-time` command must be larger than the value set by the `oadp interval-time` command.

Related commands

oadp run

oadp ignore-vlan

Specifies that any OADP frames received from the VLAN specified by the VLAN ID are to be ignored.

Syntax

To set or change information:

oadp ignore-vlan <*vlan id list*>

To delete information:

no oadp ignore-vlan

Input mode

(config)

Parameters

<*vlan id list*>

Specifies a VLAN from which received OADP frames are to be ignored.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <*vlan id list*> and the specifiable values, see *Specifiable values for parameters*.

Default behavior

Any OADP frames from all the VLAN IDs are received.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

oadp run

oadp interval-time

Specifies the interval at which the Switch sends OADP frames.

Syntax

To set or change information:

oadp interval-time <*seconds*>

To delete information:

no oadp interval-time

Input mode

`(config)`

Parameters

<*seconds*>

Specifies the sending interval (in seconds) between OADP frames sent from the Switch. OADP frames are actually sent at the interval that changes randomly from 2/3 to 3/2 of the specified value.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   5 to 254

Default behavior

The interval for sending OADP frames is 60 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The value set by the `oadp hold-time` command must be larger than the value set by the `oadp interval-time` command.

Related commands

oadp run

oadp run

Enables the OADP functionality.

Syntax

To set information:

oadp run

To delete information:

no oadp run

Input mode

(config)

Parameters

None

Default behavior

The OADP 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 29. Port Mirroring

monitor option
monitor session

monitor option

Sets the sampling factor for the port mirroring functionality. Specifying the sampling functionality for mirroring can lower the bandwidth of the mirror port.

Syntax

To set or change information:

monitor option sample <*sample count*>

To delete information:

no monitor option

Input mode

`(config)`

Parameters

sample <*sample count*>

Specifies the sampling factor for port mirroring used on the entire switch. Mirroring is performed by extracting one frame in every *n* frames, where *n* is the number of frames specified by the sampling factor.

1. Default

   This parameter cannot be omitted.

2. Range of values:

   1, 2, 8, 32, 128, 512, 2048, 8192, 32768, 131072, 524288, 2097152, 8388608, 33554432, 134217728, 536870912

   Specify 1, or a value that is 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. The following table describes the relationship between the entered value and set value.

Table 29-1: 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	1
2	2	2
5	3 to 8	8
4	9 to 32	32
5	33 to 128	128
6	129 to 512	512
7	513 to 2048	2048
8	2049 to 8192	8192
9	8193 to 32768	32768
10	32769 to 131072	131072
11	131073 to 524288	524288

#	Sampling interval entered in the command	Sampling interval actually set
12	524289 to 2097152	2097152
13	2097153 to 8388608	8388608
14	8388609 to 33554432	33554432
15	33554433 to 134217728	134217728
16	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

In port mirroring functionality, sampling is not performed, and all target frames are mirrored.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Sampling is performed randomly at a rate of one frame in *n* frames, where *n* is the number specified for the sampling factor.

Related commands

monitor session

monitor session

Configures the port mirroring functionality.

Syntax

To set or change information:

monitor session <*session no.*> source interface <*interface id list*> [{rx | tx | both}] destination interface {gigabitethernet | tengigabitethernet } <*nif no.*>/<*port no.*>

To change information:

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 191

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:

   both

2. Range of values:

   `rx`, `tx`, or `both`

destination interface {gigabitethernet | tengigabitethernet } *<nif no.>/<port no.>*

Specifies a mirror port for port mirroring. A port for which Layer 2 information has been set cannot be specified.

{gigabitethernet | tengigabitethernet}

Specifies the mirror port type.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   gigabitethernet or tengigabitethernet

<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

If an active line is specified as the mirror port, communication is no longer possible on the line. If a line is specified as the monitor port, communication is not affected.

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. Also, one monitor port can be used for both a send port mirroring session and a receive port mirroring session. However, received or sent frames copied by port mirroring 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. Regular frames cannot be sent or received on a port that has been set as a mirror port.
4. A port for which Layer 2 information has been set cannot be set as a mirror port. If you use a port for which Layer 2 information has already been set as a mirror port, delete the Layer 2 information of the applicable interface before setting the port as a mirror port.
5. A port that has already been set as a mirror port cannot be set as a monitor port.
6. If a NIF accommodating a port that has been set for a monitor port or a mirror port is replaced with another type of NIF, the corresponding port mirroring session will be 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 30. Error Messages Displayed When Editing the Configuration

30.1 Error messages displayed when editing the configuration

30.1.1 Common

See *21.1.1 Common* in the manual *Configuration Command Reference Vol. 1 For Version 11.7*.

30.1.2 Flow mode information

Table 30-1: Flow mode error messages

Message	Description
Cannot change the flow mac mode.	The MAC mode cannot be changed or set. The details are as follows: • The MAC mode cannot be changed because access lists or QoS flow lists have been set for the specified interface. Before you change the MAC mode, remove all access lists and QoS flow lists from the interface. • The MAC mode cannot be set because access lists or QoS flow lists have been set for Ethernet interfaces that belong to the specified VLAN. Before you set the MAC mode, remove all access lists and QoS flow lists from the Ethernet interfaces that belong to the specified VLAN.
Cannot set the flow mac mode, because of fldm.	The flow distribution pattern that has been set does not allow the MAC mode to be set. To set the MAC mode, specify `standard` or `extended` as the flow distribution pattern.

30.1.3 VLAN list information

Table 30-2: VLAN list error messages

Message	Description
Cannot change the VLAN list.	The specified VLAN list cannot be changed because it is specified as a detection condition in an access list or QoS flow list. Because the specified VLAN list is specified for the detection conditions of an access list or QoS flow list, if the VLAN list is changed, the VLAN IDs of the flow detection conditions are also changed. All VLAN IDs, in a VLAN list, that are conditions in an access list or QoS flow list must also be defined in the settings of the Ethernet interface to which the access or QoS flow list is applied.
Cannot delete the VLAN list.	The specified VLAN list cannot be deleted because it is specified as a detection condition in an access list or QoS flow list. Before you delete a VLAN list, delete its specification from access lists and QoS flow lists.
The maximum number of entries are exceeded.	The number of entries exceeded the capacity limit. Because the specified VLAN list is specified as a detection condition in an access list or QoS flow list, the number of entries exceeded the capacity limit when the VLAN list was changed. When you change a VLAN list, use either of the following methods: • Delete the VLAN list specification from access lists and QoS flow lists, and then change the list. • Make a change that does not cause the capacity limit to be exceeded.

30.1.4 Access list information

Table 30-3: Access list error messages

Message	Description
Cannot attach this list because flow mac mode is set.	The access list cannot be applied. The reason is described below. • If an attempt was made to apply an IPv4 or IPv6 access list to a VLAN An IPv4 or IPv6 access list cannot be applied to Layer 2 forwarding over a VLAN interface in MAC mode. Disable MAC mode before you apply an IPv4 or IPv6 access list. • If an attempt was made to apply an access list to an Ethernet interface No access list can be applied to the specified Ethernet interface because MAC mode is set for the VLAN to which the interface belongs. Before you apply an access list to an Ethernet interface, disable MAC mode for all VLANs to which the interface belongs.
Cannot attach this list because IPv6 source address prefix-length exceeds 64.	An access list containing a flow detection condition whose IPv6 source address prefix length is longer than 64 bits is invalid. The following conditions must be satisfied: • The length of the IPv6 source address prefix in a flow detection condition cannot exceed 64 bits. • The keyword `host` cannot be specified for an IPv6 source address in a flow detection condition.
Cannot change the configuration because there is an inconsistency between fwdm and policy based routing.	The configuration cannot be changed because there is an inconsistency between the allocation pattern settings for routing table entries and the policy-based routing settings. Review the configuration.
Cannot set policy based routing entry because specified destination address is invalid.	The entry cannot be set because policy-based routing does not support the destination address specified as a filtering condition. If you use IPv4 policy-based routing, for the destination address, specify an IP address that is not a multicast address, restricted broadcast address, or internal loopback address. If you use IPv6 policy-based routing, for the destination address, specify an IP address that is not a multicast address or link-local address.
Cannot set policy based routing entry because specified source address is invalid.	The entry cannot be set because policy-based routing does not support the source address specified as a filtering condition. If you use IPv4 policy-based routing, specify for the source address an IP address that is not a multicast address or internal loopback address. If you use IPv6 policy-based routing, specify for the destination address an IP address that is not a multicast address or link-local address.
Cannot set the access list logging, because hardware mode doesn't correspond to access list logging.	An access list in which `log` is specified as an action cannot be set because `system hardware-mode access-log` is not enabled. Before specifying `log` as an action in an access list, enable logging by using the `system hardware-mode` command with the `access-log` parameter.
Cannot set the configuration because there is an inconsistency between vlan and policy based switching.	The entry cannot be set because there is an inconsistency between the VLAN parameter settings for filter conditions and the policy-based switching settings. When specifying policy-based switching, specify the VLAN ID that is the same as that of the destination set in the policy-based switching list information for the filter detection conditions. Note that the VLAN list name cannot be specified
Over two entry as an address family cannot be set.	Another access list has already been applied. If you want to apply an access list, first delete the existing access list that has already been applied.
Range-Start must be less than Range-End.	The start value of a range specification is not smaller than the end value. For range specifications, make sure that the start value is smaller than the end value.

Message	Description
The maximum number of access-list entries are exceeded.	The number of access list entries exceeded the maximum. The maximum number of access list entries that can be set is 4000. To check the number of entries used in this configuration file for a specific access list, execute the `show running-config` command, and count the number of filter condition command entries in the access list. Applicable commands are as follows: • `access-list` command • `deny (ip access-list standard)` command • `deny (ip access-list extended)` command • `deny (ipv6 access-list)` command • `deny (mac access-list extended)` command • `deny (advance access-list)` command • `permit (ip access-list standard)` command • `permit (ip access-list extended)` command • `permit (ipv6 access-list)` command • `permit (mac access-list extended)` command • `permit (advance access-list)` command
The maximum number of entries are exceeded.	The number of filter entries exceeds the capacity limit. The number of used entries and available entries in the configuration file can be checked by using the `show system` command.
The maximum number of access-list and qos-flow-list entries are exceeded.	The number of access list and QoS flow list entries exceeded the maximum. The maximum number of entries that can be set as filter conditions in access lists and as flow detection conditions and actions in QoS flow lists is 32000. To check the number of entries used in this configuration file for a specific access list, execute the `show running-config` command, and count the number of filter condition command entries in the access list. To check the number of entries used in this configuration file for a specific QoS flow list, execute the `show running-config` command, and count the number of flow detection and action entries in the QoS flow list. Applicable commands are as follows: • `access-list` command • `deny (ip access-list standard)` command • `deny (ip access-list extended)` command • `deny (ipv6 access-list)` command • `deny (mac access-list extended)` command • `deny (advance access-list)` command • `permit (ip access-list standard)` command • `permit (ip access-list extended)` command • `permit (ipv6 access-list)` command • `permit (mac access-list extended)` command • `permit (advance access-list)` command • `qos (ip qos-flow-list)` command • `qos (ipv6 qos-flow-list)` command • `qos (mac qos-flow-list)` command • `qos (advance qos-flow-list)` command
This list cannot be set to the layer-2 forwarding, because the list includes TCP flag parameter.	Detection conditions in this access list cannot be applied to Layer 2 forwarding. If a TCP control flag parameter is specified as a flow detection condition in an access list, the access list cannot be applied to Layer 2 forwarding. Apply the access list to Layer 3 forwarding or modify the list so that it does not contain the above parameter as a detection condition.
This list cannot be set to the layer-2 forwarding, because the list includes tos parameter.	Detection conditions in this access list cannot be applied to Layer 2 forwarding. If the `tos` parameter is specified as a flow detection condition in an access list, the access list cannot be applied to Layer 2 forwarding. Apply the access list to Layer 3 forwarding or modify the list so that it does not contain the above parameter as a detection condition.

Message	Description
This list cannot be set to the layer-2 forwarding, because the list includes traffic-class parameter.	Detection conditions in this access list cannot be applied to Layer 2 forwarding. If a traffic class parameter is specified as a flow detection condition in an access list, the access list cannot be applied to Layer 2 forwarding. Apply the access list to Layer 3 forwarding or modify the list so that it does not contain the above parameter as a detection condition.
This list cannot be set to the outbound of this interface because this list includes 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. Delete policy-based routing entries from the access list, and then apply it to the sending side of the interface.
This list cannot be set to this interface, because the list includes own or own-address parameter.	Detection conditions in this access list cannot be applied to this interface. All of the following conditions must be satisfied: • The list must be applied to a VLAN interface. • An address must be set for the VLAN interface to which the list is applied. • Only one IPv6 global address must be set.
This list cannot be set to this interface because this list includes policy based routing entry.	This access list cannot be applied to an Ethernet interface because the access list includes policy-based routing. Delete policy-based routing entries from the access list, and then apply it to the Ethernet interface.
This list cannot be set to this interface specifying layer2-forwarding, because this list includes policy based routing entry.	This access list cannot be applied to an interface by specifying `layer2-forwarding` because the access list includes policy-based routing. Delete policy-based routing entries from the access list, and then apply it to the interface by specifying `layer2-forwarding`.
This list cannot be set to this port.	This access list cannot be applied to this Ethernet interface. To apply an access list to an Ethernet interface, the interface's settings must include the VLAN ID specified in the access list as a flow detection condition or include all VLAN IDs specified in the VLAN list.
This list cannot be set to VLAN.	This access list cannot be applied to VLAN interfaces. If a VLAN ID or VLAN list is specified as a flow detection condition in an access list, the access list cannot be applied to VLAN interfaces. Apply it to an Ethernet interface or delete the VLAN ID or VLAN list specification from the detection conditions.
This list cannot be set, because fldm prefer qos-only extended.	No access list can be applied if the flow distribution pattern is `qos-only`. To apply an access list, change the flow distribution pattern.
This list cannot be set, because of fldm.	The flow distribution pattern that has been set does not allow this list to be set. To apply an `advance access-list` to an interface, specify `standard-advance` or `extended-advance` as the flow distribution pattern.
This list cannot be set to the outbound of this interface because this list includes policy based switching entry.	This access list cannot be applied to the sending side of the interface because the access list includes policy-based switching. Delete policy-based switching entries from the access list, and then apply it to the sending side of the interface.
This list name is being used as other protocol type by other definition.	The name has already been used for another access list. Specify a name that is not being used for another access list or specify the correct name of an applicable access list.
This policy-list number is not defined.	The policy-based routing list number cannot be specified. Specify an applicable policy-based routing list number that has already been set.

Message	Description
This policy-switch-list number is not defined.	The policy-based switching list number cannot be specified. Specify an applicable policy-based switching list number that has already been set.
This vlan-list name is not defined.	The VLAN list name cannot be specified. Specify a VLAN list name that has already been set.

30.1.5 Access list logging information

Table 30-4: Access list logging error messages

Message	Description
Cannot set the access list logging, because hardware mode doesn't correspond to access list logging.	Access list logging cannot be set because `system hardware-mode access-log` is not enabled. To enable access list logging, use the `system hardware-mode` command with the `access-log` parameter.

30.1.6 QoS information

Table 30-5: QoS error messages

Message	Description
Can not set half duplex because traffic-shape rate is specified for the port.	Half duplex mode cannot be set because port bandwidth control is set for the line.
Can not set traffic-shape rate because of the port is half duplex.	Port bandwidth control cannot be set because the line is half duplex.
Cannot attach this list because flow mac mode is set.	The QoS flow list cannot be applied. The reason is described below. • If an attempt was made to apply an IPv4 or IPv6 QoS flow list to a VLAN An IPv4 or IPv6 QoS flow list cannot be applied to Layer 2 forwarding over a VLAN interface in MAC mode. Disable MAC mode before you apply an IPv4 or IPv6 QoS flow list. • If an attempt was made to apply a QoS flow list to an Ethernet interface No QoS flow list can be applied to the specified Ethernet interface because MAC mode is set for the VLAN to which the interface belongs. Before you apply a QoS flow list to an Ethernet interface, disable MAC mode for all VLANs to which the interface belongs.
Cannot attach this list because IPv6 source address prefix-length exceeds 64.	An access list containing a flow detection condition whose IPv6 source address prefix length is longer than 64 bits is invalid. The following conditions must be satisfied: • The length of the IPv6 source address prefix in a flow detection condition cannot exceed 64 bits. • The keyword `host` cannot be specified for an IPv6 source address in a flow detection condition.
Cannot change hierarchical shaper because a user is specified in a flow-qos-list.	The hierarchical shaper configuration command (`number-of-queue`, `mode`, or `shaper auto-configuration`) cannot be changed because a user ID (<*user id*>, `llrlq1`, or `llrlq2`) is set in a flow QoS configuration.
Cannot change shaper mode when there is a shaper configuration in the interface.	The shaper mode cannot be changed. For the interface with the specified NIF number, remove the shaper configuration settings at the (`config-if`) level before attempting to change the shaper mode.
Cannot change shaper number-of-queue when there is a shaper configuration in the interface.	The number of shaper queues cannot be changed. For the interface with the specified NIF number, remove the shaper configuration settings at the (`config-if`) level before attempting to change the shaper mode.

Message	Description
Cannot set hierarchical shaper and legacy shaper simultaneously.	The hierarchical shaper functionality and legacy shaper functionality cannot be set simultaneously.
Cannot set shaper nif and shaper auto-configuration simultaneously.	The automatic shaper setting functionality and shaper NIF information cannot be set simultaneously.
Cannot set the upc-storm-control mode.	The bandwidth monitoring storm control mode cannot be set because bandwidth monitoring is set for the interface. Before you set bandwidth monitoring storm control mode, delete bandwidth monitoring entries from all QoS flow lists that have been applied.
Duplicate shaper user id configuration.	An attempt was made to set a user ID that has already been set for the port. For the user ID, specify a number that has not yet been set.
Min-burst must be less than max-burst.	The minimum bandwidth burst size is not smaller than the maximum bandwidth burst size. For the minimum bandwidth burst size, set a value smaller than the maximum bandwidth burst size.
Min-rate is less than llpq-peak-rate.	The minimum bandwidth rate is smaller than the LLPQ bandwidth control value. • Range of values: <*kbit/s*>: 64 to 1000000 <*Mbit/s*>: 1 M to 1000 M
Minrate must be less than maxrate.	The minimum bandwidth rate is not smaller than the maximum bandwidth rate. For the minimum bandwidth rate, set a value smaller than the maximum bandwidth rate.
NIF does not support hierarchical shaper.	This NIF does not support the hierarchical shaper functionality.
NIF does not support legacy shaper.	This NIF does not support the legacy shaper functionality.
NIF does not support this shaper mode.	This NIF does not support this shaper mode.
Over two entry as an address family cannot be set.	Another QoS flow list has already been applied. If you want to apply a QoS flow list, first delete the existing QoS flow list that has already been applied.
Peak-rate is less than llpq-peak-rate.	The maximum bandwidth rate is smaller than the LLPQ bandwidth control value. • Range of values: <*kbit/s*>: 64 to 1000000 <*Mbit/s*>: 1 M to 1000 M
Peak-rate is less than min-rate.	The maximum bandwidth rate is smaller than the minimum bandwidth rate. • Range of values: <*kbit/s*>: 64 to 1000000 <*Mbit/s*>: 1 M to 1000 M
Range-Start must be less than Range-End.	The start value of a range specification is not smaller than the end value. For range specifications, make sure that the start value is smaller than the end value.
Relations between <*value1*> and shaper mode are inconsistent.	<*value1*> is not consistent with the shaper mode. Set `llrlq` as the shaper mode of the specified NIF.
	<*value1*>: llrlq1-burst, llrlq2-burst
Relations between <*value1*> and shaper mode are inconsistent.	<*value1*> is not consistent with the shaper mode. Set `llrlq` as the shaper mode.
	<*value1*>: llrlq1, llrlq2

Message	Description
Relations between max-psp and UPC entry are inconsistent.	The configuration cannot be changed because the number of active PSP units that is set conflicts with the setting of a QoS flow list in which bandwidth monitoring is specified. To apply a QoS flow list, in which bandwidth monitoring is specified, to the receiving side of a VLAN interface, specify `1` as the number of active PSP units in the following commands: • redundancy max-psp • schedule-power-control max-psp • adaptive-power-control max-psp
Relations between max-psp and upc-storm-control mode are inconsistent.	The configuration cannot be changed because the number of active PSP units that is set conflicts with the bandwidth storm control mode setting. To change the bandwidth storm control mode to `upc-in-out`, specify `1` as the number of active PSP units in the following commands: • redundancy max-psp • schedule-power-control max-psp • adaptive-power-control max-psp
Relations between number-of-queue and shaper mode are inconsistent.	The number of queues is not consistent with the shaper mode. If the shaper mode is `llpq4`, you cannot specify `4` as the number of queues.
Shaper mode configuration is required beforehand to set the shaper configuration to the interface.	No shaper configuration commands can be set for the interface because the shaper mode is not set for the interface. Set a shaper mode for the NIF of the specified interface.
Shaper port rate-limit is less than shaper wgq-group rate-limit.	The port bandwidth control value is smaller than the WGQ bandwidth control value. • Range of values: <*kbit/s*>: 64 to 1000000 <*Mbit/s*>: 1 M to 1000 M
Shaper port rate-limit must be greater than the peak-rate of each shaper user and peak-rate of shaper default-user.	The port bandwidth control value must be equal to or larger than the maximum bandwidth of any user and the maximum bandwidth of the default user.
Shaper port rate-limit must be greater than the sum of max-rate of llrlq1 and max-rate of llrlq2.	The port bandwidth control value must be equal to or larger than the total of the maximum bandwidths of `llrlq1` and `llrlq2`.
Shaper port rate-limit must be greater than the sum of min-rate of each shaper user, and min-rate of default-user.	The port bandwidth control value must be equal to or larger than the total of the minimum bandwidths of all users and the default user.
Shaper port rate-limit must be greater than the sum of min-rate of each shaper user, min-rate of default-user, max-rate of llrlq1, and max-rate of llrlq2.	The port bandwidth control value must be equal to or larger than the total of minimum bandwidths of all user and the default user, and the maximum bandwidths of `llrlq1` and `llrlq2`.
Specified rate value of WFQ is incorrect, or it is out of range.	The rate value specified for WFQ is either incorrect or outside the specifiable range.
Specified traffic-shape rate value is incorrect, or it is out of range.	The bandwidth rate specified for port bandwidth control is either incorrect or outside the specifiable range.
Storm-control must be with "upc-storm-control mode upc-in-and-storm-control"	The bandwidth monitoring storm control mode cannot be changed because storm control is set for the interface. • For AX6700S series switches: Before you change the bandwidth monitoring storm control mode, delete the storm control setting. • For AX6600S or AX6300S series switches: If you change the bandwidth monitoring storm control mode to `upc-in-in` or `upc-in-out`, delete the storm control setting beforehand.

Message	Description
The list cannot be applied in the inbound direction, because shaper nif configuration is missing or inconsistent among the nif ports.	A QoS flow list whose action entries contain a user ID (<*user id*>, `llrlq1`, or `llrlq2`) cannot be set on the receiving (inbound) side for either of the following reasons: The automatic shaper setting functionality is not set, or the shaper settings (shaper mode and number of shaper queues) specified for NIFs in a shaper mode on the device are not the same. Set the automatic shaper setting functionality or make sure that the shaper settings of all NIFs for which a shaper mode is set are the same.
The list cannot be applied in the outbound direction, because shaper nif configuration is missing or inconsistent among the vlan ports.	A QoS flow list whose action entries contain a user ID (<*user id*>, `llrlq1`, or `llrlq2`) cannot be set on the sending (outbound) side for either of the following reasons: The automatic shaper setting functionality is not set, or the shaper settings (shaper mode and number of shaper queues) specified for NIFs to which the interfaces included in the VLAN belong are not the same. Set the automatic shaper setting functionality. Alternatively, make sure that the NIFs to which the interfaces included in the VLAN belong satisfy the following condition: • All NIFs for which a shaper mode is set must have the same shaper settings specified.
The list cannot be applied to the interface, because the list contains user id parameter.	A list whose action entries contain a user ID (<*user id*>, `llrlq1`, or `llrlq2`) cannot be applied to this interface. The QoS flow list cannot be applied to the current shaper settings (shaper mode, number of shaper queues, and automatic shaper setting functionality): `llrlq1`, `llrlq2`, or a user ID that is not in the specifiable range is set in action entries. For details about conditions in which a user ID can be specified, see *6.4 Description of the hierarchical shaper* in the manual *Configuration Guide Vol. 2 For Version 11.7*.
The list cannot be set to the vlan interface, because the vlan has no ethernet port which is configured shaper mode.	A QoS flow list whose action entries contain a user ID (<*user id*>, `llrlq1`, or `llrlq2`) cannot be set on the sending (outbound) side for either of the following reasons: The automatic shaper setting functionality is not set, or the VLAN interface does not contain any NIF Ethernet interfaces for which a shaper mode is set. Set the automatic shaper setting functionality. Alternatively, make sure that the VLAN interface contains at least one NIF Ethernet interface for which a shaper mode is set.
The list contains user id, but shaper nif is not configured.	A QoS flow list whose action entries contain a user ID (<*user id*>, `llrlq1`, or `llrlq2`) cannot be set because the automatic shaper setting functionality or a shaper mode is not set. Set the automatic shaper setting functionality or a shaper mode.

Message	Description
The maximum number of access-list and qos-flow-list entries are exceeded.	The number of access list and QoS flow list entries exceeded the maximum. The maximum number of entries that can be set as filter conditions in access lists and as flow detection conditions and actions in QoS flow lists is 32000. To check the number of entries used in this configuration file for a specific access list, execute the `show running-config` command, and count the number of filter condition command entries in the access list. To check the number of entries used in this configuration file for a specific QoS flow list, execute the `show running-config` command, and count the number of flow detection and action entries in the QoS flow list. Applicable commands are as follows: • `access-list` command • `deny (ip access-list standard)` command • `deny (ip access-list extended)` command • `deny (ipv6 access-list)` command • `deny (mac access-list extended)` command • `deny (advance access-list)` command • `permit (ip access-list standard)` command • `permit (ip access-list extended)` command • `permit (ipv6 access-list)` command • `permit (mac access-list extended)` command • `permit (advance access-list)` command • `qos (ip qos-flow-list)` command • `qos (ipv6 qos-flow-list)` command • `qos (mac qos-flow-list)` command • `qos (advance qos-flow-list)` command
The maximum number of entries are exceeded.	The number of QoS entries exceeds the capacity limit. The number of used entries and available entries in the configuration can be checked by using the `show system` command.
The maximum number of qos-flow-list entries are exceeded.	The number of QoS flow list entries exceeded the maximum. The maximum number of entries that can be set as flow detection conditions and actions in QoS flow lists is 4000. To check the number of entries used in this configuration file for a specific QoS flow list, execute the `show running-config` command, and count the number of flow detection and action entries in the QoS flow list. Applicable commands are as follows: • `qos (ip qos-flow-list)` command • `qos (ipv6 qos-flow-list)` command • `qos (mac qos-flow-list)` command • `qos (advance qos-flow-list)` command
The maximum number of shaper user entries is exceeded.	The number of shaper user entries exceeds the capacity limit.
The maximum rate for the queue is inconsistent with the other queue's rate.	The total of the maximum send bandwidths of all queues exceeds 100%. Alternatively, the maximum send bandwidth rate for a higher queue number is smaller than the maximum send bandwidth rate for a lower queue number. Make sure that the total of the maximum send bandwidths of all queues does not exceed 100%, and that the maximum send bandwidth rate for a lower queue number does not exceed that for a higher queue number.
The unit of the specified traffic-shape rate is unjustified.	The specified port bandwidth increment is invalid.
This list cannot be set to the inbound, because upc-storm-control mode <*upc-storm-control mode*>.	If the bandwidth monitoring storm control mode is not `upc-in-in`, the maximum bandwidth control and minimum bandwidth monitoring cannot be set simultaneously on the receiving side. To set both maximum bandwidth control and minimum bandwidth monitoring for a flow detection condition, change the bandwidth monitoring storm control mode.

Message	Description
	<*upc-storm-control mode*>: • For AX6700S series switches: upc-in-and-storm-control • For AX6600S or AX6300S series switches: upc-in-and-storm-control, upc-in-out
This list cannot be set to the layer-2 forwarding, because the list includes replace-dscp or penalty-dscp parameter.	Action entries in this QoS flow list cannot be applied to Layer 2 forwarding. If action entries in a QoS flow list contain `replace-dscp` or `penalty-dscp`, the QoS flow list cannot be applied to Layer 2 forwarding. Apply the list to Layer 3 forwarding over a VLAN interface. Alternatively, do not specify `replace-dscp` or `penalty-dscp`.
This list cannot be set to the layer-2 forwarding, because the list includes TCP flag parameter.	Detection conditions in this QoS flow list cannot be applied to Layer 2 forwarding. If a TCP control flag parameter is specified as a flow detection condition in a QoS flow list, the QoS flow list cannot be applied to Layer 2 forwarding. Apply the access list to Layer 3 forwarding or modify the list so that it does not contain the above parameter as a detection condition.
This list cannot be set to the layer-2 forwarding, because the list includes tos parameter.	Detection conditions in this QoS flow list cannot be applied to Layer 2 forwarding. If the `tos` parameter is specified as a flow detection condition in a QoS flow list, the QoS flow list cannot be applied to Layer 2 forwarding. Apply the access list to Layer 3 forwarding or modify the list so that it does not contain the above parameter as a detection condition.
This list cannot be set to the layer-2 forwarding, because the list includes traffic-class parameter.	Detection conditions in this QoS flow list cannot be applied to Layer 2 forwarding. If a traffic class is set as a flow detection condition in a QoS flow list, the QoS flow list cannot be applied to Layer 2 forwarding. Apply the access list to Layer 3 forwarding or modify the list so that it does not contain the above parameter as a detection condition.
This list cannot be set to the outbound, because it includes a flow entry which sets both the maxrate and the minrate.	Maximum bandwidth control and minimum bandwidth monitoring cannot be set simultaneously for the flow detection condition on the sending side. Modify the QoS flow list so that either maximum bandwidth control or minimum bandwidth monitoring is specified for the flow detection condition.
This list cannot be set to the outbound, because it includes the UPC entry.	Bandwidth monitoring cannot be performed on the sending side. Bandwidth monitoring can be performed only on the receiving side.
This list cannot be set to the outbound, because upc-storm-control mode <*upc-storm-control mode*>.	Bandwidth monitoring cannot be performed on the sending side if the bandwidth monitoring storm control mode is `upc-in-and-storm-control` or `upc-in-in`. To perform bandwidth monitoring on the sending side, change the bandwidth monitoring storm control mode.
	<*upc-storm-control mode*>: upc-in-and-storm-control, upc-in-in
This list cannot be set to the VLAN interface, because it includes the UPC entry.	Bandwidth monitoring cannot be performed for a VLAN interface. Bandwidth monitoring can be performed for only an Ethernet interface.
This list cannot be set to this interface, because the list includes own or own-address parameter.	Detection conditions in this QoS flow list cannot be applied to this interface. All of the following conditions must be satisfied: • The list must be applied to a VLAN interface. • An address must be set for the VLAN interface to which the list is applied. • Only one IPv6 global address must be set.
This list cannot be set to this port.	This QoS flow list cannot be applied to this Ethernet interface. To apply a QoS flow list to an Ethernet interface, the interface's settings must include the VLAN ID specified in the QoS flow list as a flow detection condition or include all VLAN IDs specified in the VLAN list.

Message	Description
This list cannot be set to VLAN.	This QoS flow list cannot be applied to VLAN interfaces. If a VLAN ID or VLAN list is set as a flow detection condition in a QoS flow list, the QoS flow list cannot be applied to VLAN interfaces. Apply the list to an Ethernet interface or delete the VLAN ID or VLAN list settings from the detection conditions.
This list cannot be set, because fldm prefer filter-only extended.	No QoS flow list can be applied if the flow distribution pattern is `filter-only`. To apply a QoS flow list, change the flow distribution pattern.
This list cannot be set, because of fldm.	The flow distribution pattern that has been set does not allow this list to be set. To apply an `advance qos-flow-list` to an interface, specify `standard-advance` or `extended-advance` as the flow distribution pattern.
This list name is being used as other protocol type by other definition.	The name has already been used for another QoS flow list. Specify a name that is not being used for another QoS flow list or specify the correct name of an applicable QoS flow list.
This vlan-list name is not defined.	The VLAN list name cannot be specified. Specify a VLAN list name that has already been set.

30.1.7 IEEE 802.1X information

Table 30-6: IEEE 802.1X error messages

Message	Description
ChGr <*channel group number*>: Inconsistency is found between the dot1x port-control and the dot1x vlan <*vlan id*> enable configuration.	Per-VLAN VLAN-based static authentication is inconsistent with port-based authentication of channel groups. If VLAN-based authentication (static) is set for a VLAN, port-based authentication cannot be set for channel groups that belong to the VLAN. If port-based authentication is set for a channel group, VLAN-based authentication (static) cannot be set for a VLAN to which the channel group belongs.
	<*channel group number*>: Indicates the channel group number. <*vlan id*>: Indicates the VLAN ID.
ChGr <*channel group number*>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	Port-based authentication channel groups and Layer 2 interface attributes do not match. If port-based authentication channel groups are used, then the only switchport mode that can be set is `access`. Conversely, if the `switchport mode` command is used to set a mode other than `access` for a channel group, then port-based authentication cannot be used.
	<*channel group number*>: Indicates the channel group number.
ChGr <*channel group number*>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	For port-based authentication of channel groups, the `ignore-eapol-start` and `reauthentication` settings must be consistent. If `reauthentication` is not set, then `ignore-eapol-start` cannot be set. Set `reauthentication` first, then set `ignore-eapol-start`.
	<*channel group number*>: Indicates the channel group number.

Message	Description
ChGr <*channel group number*>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	For port-based authentication of channel groups, the `ignore-eapol-start` and `supplicant-detection` settings must be consistent. If `ignore-eapol-start` is set, then `supplicant-detection` cannot be set to `disable`. Conversely, if `supplicant-detection` is disabled, then `ignore-eapol-start` cannot be set.
	<*channel group number*>: Indicates the channel group number.
Inconsistency is found between the dot1x and the fense configuration.	The IEEE 802.1X configuration is inconsistent with the authentication VLAN configuration. The `dot1x system-auth-control` command cannot be set together with any of the following commands: • fense vaa-name • fense vlan • fense server
Inconsistency is found between the dot1x and the gsrp configuration.	The IEEE 802.1X configuration is inconsistent with the GSRP configuration. The `dot1x system-auth-control` command and the `gsrp` command cannot be set simultaneously.
Inconsistency is found between the dot1x and the l2protocol-tunnel eap configuration.	The IEEE 802.1X configuration is inconsistent with the EAPOL forwarding configuration. You cannot set both port-based authentication and a VLAN that uses EAPOL forwarding for the same port or channel group. You cannot set both VLAN-based authentication (static or dynamic) and EAPOL forwarding for the same VLAN.
Inconsistency is found between the dot1x and the mac-address-table limit configuration.	The IEEE 802.1X configuration is inconsistent with the restriction of MAC address learning. You cannot set both IEEE 802.1X and the restriction of MAC address learning for the same port, channel group, or VLAN.
Inconsistency is found between the dot1x and the no mac-address-table learning configuration.	The IEEE 802.1X configuration is inconsistent with the suppression of MAC address learning. You cannot set both port-based authentication and a VLAN that uses suppression of MAC address learning for the same port or channel group. You cannot set both VLAN-based authentication (static or dynamic) and the suppression of MAC address learning for the same VLAN.
Inconsistency is found between the dot1x vlan enable and the switchport mode configuration.	VLAN-based authentication (static) is inconsistent with a Layer 2 interface attribute. You cannot set VLAN-based authentication (static) for a VLAN to which a tunneling port belongs.
Inconsistency is found between the dot1x vlan enable or dot1x vlan dynamic radius-vlan <*vlan id*> and the vlan configuration.	VLAN-based authentication (static or dynamic) is inconsistent with the VLAN configuration. You cannot delete a VLAN for which VLAN-based authentication (static or dynamic) has been set. Delete the VLAN-based authentication (static or dynamic) settings from the VLAN, and then delete the VLAN.
	<*vlan id*>: Indicates the VLAN ID.
Inconsistency is found between the vrf and the dot1x configuration.	The IEEE 802.1X configuration is inconsistent with the VRF configuration. The `dot1x system-auth-control` command and the `vrf mode` command cannot be set simultaneously.

Message	Description
port <*nif no.*>/<*port no.*>: Inconsistency is found between the dot1x port-control and the dot1x vlan <*vlan id*> enable configuration.	VLAN-based authentication (static) is inconsistent with port-based authentication. If VLAN-based authentication (static) is set for a VLAN, port-based authentication cannot be set for ports that belong to the VLAN. If port-based authentication is set for a port, VLAN-based authentication (static) cannot be set for a VLAN to which the port belongs.
	<*nif no.*>/<*port no.*>: Indicates the NIF number/port number. <*vlan id*>: Indicates the VLAN ID.
port <*nif no.*>/<*port no.*>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	Port-based authentication channel groups and Layer 2 interface attributes do not match. If port-based authentication of a port is used, then the only switchport mode that can be set for the port is `access`. Conversely, if the `switchport mode` command is used to set a mode other than `access` for a port, then port-based authentication cannot be used.
	<*nif no.*>/<*port no.*>: Indicates the NIF number/port number.
port <*nif no.*>/<*port no.*>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	For port-based authentication of ports, the `ignore-eapol-start` and `reauthentication` settings must be consistent. If `reauthentication` is not set, then `ignore-eapol-start` cannot be set. Set `reauthentication` first, then set `ignore-eapol-start`.
	<*nif no.*>/<*port no.*>: Indicates the NIF number/port number.
port <*nif no.*>/<*port no.*>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	For port-based authentication of ports, the `ignore-eapol-start` and `supplicant-detection` settings must be consistent. If `ignore-eapol-start` is set, then `supplicant-detection` cannot be set to `disable`. Conversely, if `supplicant-detection` is disabled, then `ignore-eapol-start` cannot be set.
	<*nif no.*>/<*port no.*>: Indicates the NIF number/port number.
The total count of dot1x vlan definitions is beyond the maximum value (1024).	The number of VLANs for which VLAN-based authentication (static or dynamic) is set exceeds the maximum. Make sure that the number does not exceed the maximum (1024).
The total count of dot1x vlan ports and port-channel combined is beyond the maximum value (1024).	The total number of ports and channel groups belonging to a VLAN that has VLAN-based authentication (static or dynamic) exceeds the maximum. Make sure that the number does not exceed the maximum (1024).
vlan <*vlan id*>: Inconsistency is found between the dot1x vlan enable and the switchport configuration.	The VLAN using VLAN-based authentication (static) is inconsistent with a protocol-based VLAN port or MAC VLAN port. For a VLAN using VLAN-based authentication (static), you cannot use the `switchport protocol-vlan` command to set a protocol-based VLAN as a native VLAN. You also cannot use the `switchport mac-vlan` command to set a MAC VLAN as a native VLAN. You cannot set VLAN-based authentication (static) for a protocol-based VLAN set as a native VLAN by using the `switchport protocol-vlan` command or a MAC VLAN set as a native VLAN by using the `switchport mac-vlan` command.
	<*vlan id*>: Indicates the VLAN ID.
vlan <*vlan id*>: Inconsistency is found between the dot1x vlan enable and the vlan configuration.	VLAN-based authentication (static) is inconsistent with the VLAN configuration. A VLAN that is configured to use VLAN-based authentication (static) is not set as a port VLAN by using the `vlan` command. Before you configure a VLAN to use VLAN-based authentication (static), use the `vlan` command to set the VLAN as a port VLAN.

Message	Description
	<*vlan id*>: Indicates the VLAN ID.
vlan <*vlan id*>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	For a VLAN that uses VLAN-based authentication (static), the `ignore-eapol-start` and `reauthentication` settings must be consistent. If `reauthentication` is not set, then `ignore-eapol-start` cannot be set. Set `reauthentication` first, then set `ignore-eapol-start`.
	<*vlan id*>: Indicates the VLAN ID.
vlan <*vlan id*>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	For a VLAN that uses VLAN-based authentication (static), the `ignore-eapol-start` and `supplicant-detection` settings must be consistent. If `ignore-eapol-start` is set, then `supplicant-detection` cannot be set to `disable`. Conversely, if `supplicant-detection` is disabled, then `ignore-eapol-start` cannot be set.
	<*vlan id*>: Indicates the VLAN ID.
vlan dynamic: Inconsistency is found between the radius-vlan <*vlan id*> and the vlan configuration.	VLAN-based authentication (dynamic) is inconsistent with the VLAN configuration. A VLAN that is configured to use VLAN-based authentication (dynamic) was not set as a MAC VLAN by using the `vlan` command. Before you configure a VLAN to use VLAN-based authentication (dynamic), use the `vlan` command to set the VLAN as a MAC VLAN.
	<*vlan id*>: Indicates the VLAN ID.
vlan dynamic: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	For a VLAN that uses VLAN-based authentication (dynamic), the `ignore-eapol-start` and `reauthentication` settings must be consistent. If `reauthentication` is not set, then `ignore-eapol-start` cannot be set. Set `reauthentication` first, then set `ignore-eapol-start`.
vlan dynamic: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	For a VLAN that uses VLAN-based authentication (dynamic), the `ignore-eapol-start` and `supplicant-detection` settings must be consistent. If `ignore-eapol-start` is set, then `supplicant-detection` cannot be set to `disable`. Conversely, if `supplicant-detection` is disabled, then `ignore-eapol-start` cannot be set.

30.1.8 Web authentication information

Table 30-7: Web authentication error messages

Message	Description
Duplicate IP address.	The same IP address has already been used. Specify an IP address that has not been used for an interface or local address.
Duplicate network address.	An address included in the subnet set for an interface is set as a Web authentication IP address.
Duplicate web authentication port number.	The same Web authentication port number is used more than once. Eliminate duplication of Web authentication port numbers.
Inconsistency is found between the VAA configuration and the web-authentication configuration.	The Web authentication start command cannot be executed if the `FENSE` command has been set.

Message	Description
Inconsistency is found between the vrf and the web-authentication configuration.	The Web authentication start command cannot be executed if the `vrf mode` command has been set.
Inconsistency is found between the web-authentication vlan command and web-authentication port command.	Legacy mode setting and dynamic or fixed VLAN mode setting cannot co-exist on the same device.
Invalid access-list ID for authentication.	Only one authentication access list can be set per device.
Invalid max-timer . -- <*value*>	The maximum connection time is outside the valid range. Set a value from 10 to 1440 or the literal `infinity`.
	<*value*>: Indicates the maximum connection time for Web authentication.
Invalid max-user . -- <*value*>	The maximum number of concurrent users is outside the valid range. Set a value from 1 to 4096.
	<*value*>: Indicates the maximum number of concurrent users for Web authentication.
Invalid vlan . -- <*value*>	The VLAN ID is outside the valid range. Set a value from 2 to 4095.
	<*value*>: Indicates the VLAN ID of the VLAN after Web authentication or the VLAN ID of the URL redirection VLAN for Web authentication.
Invalid VLAN ID <*vlan id*>, not MAC VLAN	The VLAN ID you set is not the ID of a MAC VLAN.
	<*vlan id*>: Indicates the VLAN ID of the post-authentication VLAN.
Maximum number of web authentication port is exceeded.	The maximum number of Web authentication port numbers that can be added is two (in total for HTTP and HTTPS). When you add Web authentication port numbers, add a maximum of two port numbers in total for HTTP and HTTPS.
Over two entry as an address family cannot be set.	Another access list has already been applied. If you want to apply an access list, first delete the existing access list that has already been applied.
Relations between the vlan configuration and the web-authentication redirect-vlan configuration are inconsistent.	When you specify the VLAN ID of a VLAN for which URL redirection is to be enabled, do not specify the VLAN ID of a MAC VLAN.
Relations between the web-authentication configuration and the channel-group configuration within same port.	A port channel configuration and a Web authentication configuration cannot be set for the same port.
Relations between the web-authentication configuration and the VLAN mode configuration are inconsistent.	Web authentication cannot be set for a port whose VLAN mode is either tunneling mode or protocol-based VLAN mode.
Relations between the web-authentication dynamic VLAN mode and the web-authentication static VLAN mode are inconsistent.	Web authentication configurations specifying different modes (fixed and dynamic VLAN modes) cannot co-exist on the same device.
Relations between the web-authentication logout polling configuration is inconsistent.	Processing cannot continue because there are inconsistencies between configurations for the Web authentication polling functionality.
Relations between web-authentication configuration and l2protocol-tunnel eap configuration are inconsistent.	URL redirection for Web authentication and EAPOL forwarding cannot be set simultaneously on the same device.

30.1.9 MAC-based authentication information

Table 30-8: MAC-based authentication error messages

Message	Description
Inconsistency is found between the VAA configuration and the mac-authentication configuration.	The MAC-based authentication activation command cannot be executed if the `FENSE` command has been set.
Inconsistency is found between the vrf and the mac-authentication configuration.	The MAC authentication activation command cannot be executed if the `vrf mode` command has been set.
Relations between the mac-authentication configuration and the channel-group configuration within same port.	A port channel configuration and a MAC-based authentication configuration cannot be set for the same port.
Relations between the mac-authentication configuration and the VLAN mode configuration are inconsistent.	MAC-based authentication cannot be set for a port whose VLAN mode is either tunneling mode or protocol-based VLAN mode.
Relations between the mac-authentication configuration and the web-authentication dynamic VLAN configuration are inconsistent.	Configurations specifying legacy mode for MAC-based authentication and Web authentication cannot co-exist on the same device.

30.1.10 Authentication VLAN information [OP-VAA]

Table 30-9: Authentication VLAN error messages

Message	Description
fense: duplicate server address <*server address*>.	The IP address set in the `fense server` command is the same as the IP address set for another VAA ID.
	<*server address*>: Indicates the IP address of an authentication server.
fense: duplicate vlan subnet address <*subnet address*> and subnet mask <*subnet mask*>.	That subnet address and mask have already been set elsewhere.
	<*subnet address*>: Indicates the subnet address of an authenticated VLAN. <*subnet mask*>: Indicates the subnet mask of an authenticated VLAN.
fense: Inconsistency is found between the dot1x and the fense configuration.	Authentication VLAN-related commands cannot be executed if IEEE 802.1X command `dot1x system-auth-control` has been set.
fense: Inconsistency is found between the vlan suspend the fense vlan configuration.	The MAC VLAN used for an authentication VLAN cannot be suspended. Conversely, a suspended MAC VLAN cannot be used for an authentication VLAN.
fense: the set of VLAN ID <*vlan id*> and subnet is different from configured set.	The subnet you set for a VLAN ID is different from the subnet that has already been set for the VLAN ID. The subnet corresponding to a VLAN ID must not change for a VAA ID.
	<*vlan id*>: Indicates the VLAN ID of an authenticated VLAN.
Inconsistency is found between the vrf and the fense configuration.	Authentication VLAN-related start commands cannot be executed if the `vrf mode` command has been set.

30.1.11 DHCP snooping information

Table 30-10: DHCP snooping error messages

Message	Description
Cannot change the configuration because there is an inconsistency between fldm and ip dhcp snooping.	The configuration cannot be changed because there is an inconsistency between DHCP snooping and flow distribution pattern settings. DHCP snooping can be set only when the following parameters are not specified in the flow distribution pattern settings: • fldm prefer default standard • fldm prefer {default | filter-only | qos-only | filter | qos} extended • fldm prefer qos-only extended-advance
Cannot change the DHCP snooping, because the maximum number of entries are exceeded.	If the DHCP snooping settings are changed, the capacity limit will be exceeded. Before you change the DHCP snooping settings, ensure that the number of flow entries that have been set will not exceed the capacity limit after the settings are changed.
The VLAN target of the DHCP snooping and ARP inspection is not suitable.	The target VLAN settings for DHCP snooping and dynamic ARP inspection are invalid. The target VLAN for dynamic ARP inspection must be a VLAN subject to DHCP snooping.

30.1.12 BSU, PSP, and NIF redundancy information [AX6700S] [AX6600S]

Table 30-11: BSU, PSP, and NIF redundancy error messages

Message	Description
Cannot change <*value1*> configuration while "power-control" or "system recovery" exist.	Either the `power-control` or `system recovery` command has already been set. <*value1*> could not be set. Delete the `power-control` or `system recovery` command. Alternatively, check whether the expected entry has already been set.
	<*value1*>: Indicates a command name.
Cannot change <*value1*> configuration while "redundancy bsu-load-balancing smac" or "redundancy bsu-mode fixed" exist.	The `redundancy bsu-load-balancing smac` command or the `redundancy bsu-mode fixed` command has already been set. <*value1*> could not be changed. Delete the `redundancy bsu-load-balancing smac` command or the `redundancy bsu-mode fixed` command. Alternatively, check whether the expected entry has already been set.
	<*value1*>: Indicates a command name.
Cannot set <*value1*> configuration while "schedule-power-control mode" or "schedule-power-control max-bsu" or "schedule-power-control standby-bsu" or "schedule-power-control time-range" or "adaptive-power-control enable" exist.	The `schedule-power-control mode`, `schedule-power-control max-bsu`, `schedule-power-control standby-bsu`, `schedule-power-control time-range`, or `adaptive-power-control enable` command has already been set. <*value1*> could not be set. Delete the `schedule-power-control mode`, `schedule-power-control max-bsu`, `schedule-power-control standby-bsu`, `schedule-power-control time-range`, or `adaptive-power-control enable` command. Alternatively, check whether the expected entry has already been set.
	<*value1*>: Indicates a command name.

Message	Description
Cannot set nif<*value1*>, because nif<*value1*> is already configured in redundancy nif group.	The indicated NIF (`nif` <*value1*>) cannot be set because it has already been set for this NIF redundancy group. Delete the NIF redundancy group settings from the NIF (`nif` <*value1*>). Alternatively, check whether the expected entry has already been set.
	<*value1*>: Indicates the suffix of the NIF number that you attempted to set.
Cannot set nif<*value1*>, because the maximum number of nif exist in this redundancy nif group.	The NIF (`nif` <*value1*>) could not be set because the number of NIFs that have been set for this redundancy group has already reached the maximum. Check the maximum number of NIFs that can be set per NIF redundancy group.
	<*value1*>: Indicates the suffix of the NIF number that you attempted to set.
Relations between redundancy max-psp and UPC entry are inconsistent.	The configuration cannot be changed because the number of active PSP units that is set conflicts with the setting of a QoS flow list in which bandwidth monitoring is specified. To change the number of active PSP units, delete QoS flow lists in which bandwidth monitoring for the receiving-side VLAN interface is specified.
Relations between redundancy max-psp and upc-storm-control mode are inconsistent.	The configuration cannot be changed because the number of active PSP units that is set conflicts with the bandwidth storm control mode setting. To change the number of active PSP units, specify either `upc-in-in` or `upc-in-and-storm-control` as the bandwidth monitoring storm control mode.

30.1.13 GSRP information

Table 30-12: GSRP error messages

Message	Description
can not configure gsrp when spanning-tree is configured.	GSRP cannot be set because the Spanning Tree Protocol has been set.
can not configure gsrp when virtual-router is configured.	GSRP cannot be set because VRRP has been set.
gsrp-<*gsrp group id*>: can not configure layer3-redundancy when GSRP ID is not in range from 1 to 4.	The `layer3-redundancy` command cannot be set if the GSRP group ID is not 1, 2, 3, or 4. Set a value from 1 to 4 for the GSRP group ID.
	<*gsrp group id*>: Indicates the GSRP group ID.
gsrp-<*gsrp group id*>: can not specify both any flush methods and direct-link on the channel-group <*channel group number*>.	You cannot specify `reset-flush-port` or `no-flush-port` for a channel group that has been specified in the direct link settings. Either delete the channel group from the relevant settings or use another channel group.
	<*gsrp group id*>: Indicates the GSRP group ID. <*channel group number*>: Indicates the channel group number.
gsrp-<*gsrp group id*>: can not specify both any flush methods and direct-link on the port <*nif no.*>/<*port no.*>.	You cannot specify `reset-flush-port` or `no-flush-port` for a port that has been specified in the direct link settings. Either delete the port from the relevant settings or use another port.
	<*gsrp group id*>: Indicates the GSRP group ID. <*nif no.*>/<*port no.*>: Indicates the NIF number/port number.

Message	Description
gsrp-<*gsrp group id*>:can not specify the two or more flush methods on the channel-group <*channel group number*>.	Two or more flush methods cannot be specified for one channel group. Either delete the channel group from the relevant settings or use another channel group.
	<*gsrp group id*>: Indicates the GSRP group ID. <*channel group number*>: Indicates the channel group number.
gsrp-<*gsrp group id*>:can not specify the two or more flush methods on the port <*nif no.*>/<*port no.*>.	Two or more flush methods cannot be specified for one port. Either delete the port from the relevant settings or use another port.
	<*gsrp group id*>: Indicates the GSRP group ID. <*nif no.*>/<*port no.*>: Indicates the NIF number/port number.
gsrp-<*gsrp group id*>-<*vlan group id*> is already configured in vlan-mapping.	The specified VLAN group ID has already been set as a VLAN mapping ID. Either delete the VLAN mapping ID from the Ring Protocol settings or use another VLAN group ID.
	<*gsrp group id*>: Indicates the GSRP group ID. <*vlan group id*>: Indicates the VLAN group ID.
gsrp-<*gsrp group id*>-<*vlan group id*>: vlan <*vlan id*> has been configured in another vlan-group.	The specified VLAN has already been set for another VLAN group. Either delete the VLAN from the other VLAN group or use another VLAN.
	<*gsrp group id*>: Indicates the GSRP group ID. <*vlan group id*>: Indicates the VLAN group ID. <*vlan id*>: Indicates the VLAN ID.
Inconsistency is found between the vrf mode and the gsrp configuration.	With the operation of VRF functionality, the command cannot be set for either of the following reasons: • GSRP cannot be set because the `vrf mode` is other than `gsrp-enable-ipv4-ipv6`. • When there is a GSRP configuration, the `vrf mode` command cannot be used to set a mode other than `gsrp-enable-ipv4-ipv6`.

30.1.14 VRRP information

Table 30-13: VRRP error messages

Message	Description
Cannot configure vrrp when gsrp is configured.	VRRP cannot be set because GSRP has been set.
Cannot follow Follow virtual router.	The virtual router you attempted to set as a follower router has already been set as a primary router. Before you specify a virtual router as a follower virtual router, make sure that the virtual router is not currently a primary router.
Cannot set mode because the virtual router set other mode.	Two or more VRRP operation modes cannot be set concurrently.
Cannot set virtual router IP address because the other one of different address family already set.	The virtual IP address cannot be set because a virtual IP address of a different address family has already been set.
Failure detection times is greater than check trial times.	The `failure detection times` value exceeds the `check trial times` value. Set a value that is no more than the `check trial times` value.

Message	Description
Follow virtual router cannot become the address owner.	A follower virtual router cannot become an address owner. When setting up VRRP, assigning IP addresses to interfaces, and assigning a virtual IP to primary (master) and follower routers, the follower router must not be the address owner.
Invalid virtual router IPv6 address. -- <*value1*>	The virtual IPv6 address is invalid.
Network address of VRRP virtual router ip address and IP address is different on accept mode.	The network addresses of the VRRP virtual and real IP addresses are different. When specifying accept mode or if accept mode has already been specified, virtual and real IP network addresses must match.
Network prefix of VRRP virtual router ipv6 address and IPv6 address is different on accept mode.	The network prefixes of the VRRP virtual and real IPv6 addresses are different. When specifying accept mode or if accept mode has already been specified, the network prefixes of the virtual and real IPv6 addresses must match.
Not found channel-group <*channel group number*>.	The specified channel group has not been set.
	<*channel group number*>: Indicates the channel group number.
Only one track can assign for virtual router with priority mode.	Only one priority switching track can be assigned to a virtual router.
Only priority mode or decrement mode can specify as priority operation method at one virtual router.	You cannot specify both priority switching and priority decrement modes for a virtual router.
Recovery detection times is greater than check trial times.	The `recovery detection times` value is greater than the `check trial times` value. Set a value that is no more than the `check trial times` value.
The number of critical interfaces for virtual router is beyond limitation.	The number of `Critical Interface` settings per virtual router is above the maximum.
The number of Primary virtual routers exceeds limit.	The number of primary virtual routers is above the maximum.

30.1.15 Storm control information

Table 30-14: Storm control error messages

Message	Description
"storm-cotorol level 0" and "storm-cotorol action" are inconsistent.	The receiver bandwidth threshold value for triggering storm control cannot be 0 when setting `storm-control action`.
Storm-control must be with "upc-storm-control mode upc-in-and-storm-control"	To enable storm control, set `upd-in-and-storm-control` using the `upc-storm-control mode` command.
Definition of "storm-cotorol action" must be same in Channel-Group.	The storm-control action settings within the same channel group must be the same.

30.1.16 CFM information

Table 30-15: CFM error messages

Message	Description
Cannot change cfm domain direction.	The MEP direction that is set in a domain cannot be changed.
Cannot change cfm mep direction.	The MEP direction cannot be changed.

Message	Description
Cannot configure cfm enable to channel-group port.	CFM of an interface participating in a port channel cannot be enabled.
Cannot configure cfm mep to channel-group port.	An MEP cannot be set for an interface that is participating in a port channel.
Cannot configure cfm mip to channel-group port.	An MIP cannot be set for an interface that is participating in a port channel.
Domain level <*level*> is set with a value less than cfm mep.	A value equal to or smaller than the value set for the MEP is specified for the specified domain level.
	<*level*>: Indicates the domain level.
Domain level <*level*> is set with values more than cfm mip.	A value equal to or greater than the value set for MIP is specified for the specified domain level.
	<*level*>: Indicates the domain level.
MA <*no.*> is already configured in cfm domain.	The specified MA identification number is already being used by another domain.
	<*no.*>: Indicates the MA identification number.
MA name <*name*> is already configured in cfm domain.	The specified MA name is already set in the same domain.
	<*name*>: Indicates the MA name.
Maximum number of cfm mep are already defined.	The number of MEP settings exceeds the maximum. Delete unnecessary MEP settings.
Maximum number of cfm mip are already defined.	The number of MIP settings exceeds the maximum. Delete unnecessary MIP settings.
MEP ID <*mepid*> is already configured in cfm mep.	The specified MEP ID has already been set for another MEP.
	<*mepid*>: Indicates the MEP ID
Not found VLAN ID <*vlan id*> in MA.	The specified VLAN ID does not exist. Specify a VLAN ID that has already been set in the MA.
	<*vlan id*>: Indicates the VLAN ID.
VLAN ID <*vlan id*> is already configured in MA name.	The specified VLAN ID is already being used by another MA name.
	<*vlan id*>: Indicates the VLAN ID.

30.1.17 SNMP information

Table 30-16: SNMP error messages

Message	Description
Group information exceeded 50 entries. <*group name*>	The number of entries specified as group information exceeded 50. Delete unnecessary entries, and then add the new one.
	<*group name*>: Indicates the group name.
Informs is supported by only SNMPv2C.	The inform function is supported by SNMPv2C. Select SNMPv2C to use the inform function.
Invalid oid-tree. <*oid tree*>	The value for <*oid tree*> is invalid. For <*oid tree*>, specify an object identifier in dot notation.

Message	Description
	<*oid tree*>: Indicates subtree information.
MIB view exceeded 50 entries. <*view name*>	The number of MIB view entries exceeded 50. Delete unnecessary MIB view entries, and then add the new one.
	<*view name*>: Indicates the MIB view name.
RMON alarm rising threshold is less than falling threshold.	The upper threshold value is less than the lower threshold value. The upper threshold value must be equal to or larger than the lower threshold value.
Subtree of the same MIB view exceeded 30 entries. <*view name*> <*oid tree*>	The number of subtrees in one MIB view exceeded 30. Delete unnecessary subtrees, and then add the new one.
	<*view name*>: Indicates the MIB view name. <*oid tree*>: Indicates subtree information.

30.1.18 sFlow statistics

Table 30-17: sFlow statistics error messages

Message	Description
Maximum number of entries are already defined.	The number of collectors that have been set exceeds the maximum. The number of collectors that have been set must not exceed four.
The sampling interval value must be set to a value that is higher than 2 when the "sflow forward egress" command enabled.	When you use the `sflow forward egress` command, the sampling interval value must be 2 or larger.

30.1.19 OADP information

Table 30-18: OADP error messages

Message	Description
Invalid parameter, hold-time must be longer than interval-time.	The value set by the `oadp interval-time` command is inconsistent with that set by the `oadp hold-time` command. • If this message is output when setting `oadp interval-time` The value set by this command is larger than the value set by the `oadp hold-time` command. • If this message is output when setting `oadp hold-time` The value set by this command is smaller than the value set by the `oadp interval-time` command.

30.1.20 Port mirroring information

Table 30-19: Port mirroring error messages

Message	Description
Mirror port and monitor port are inconsistent.	Both mirror port and monitor port settings cannot be specified simultaneously.
Mirror port and switchport are inconsistent.	Both mirror port and switchport settings cannot be specified simultaneously.
Monitor port can be specified only in one monitor session, or in a pair of one tx session and one rx session.	A monitor port can be set only for either one monitor session or one combination sending and receiving port mirroring session.

Index

G

H

I

L

M

N

O

W