AX3660S Software Manual

Configuration Command Reference Vol. 1

For Version 12.1 Rev.11

AX38S-S013X-C0

AlaxalA

■ **Relevant products**

This manual applies to the models in the AX3660S series of switches. It also describes the function of OS-L3M version 12.1 of the software.

■ **Precautions in exporting**

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. If you require more information, please contact an Alaxala sales representative.

■ **Trademarks**

AMD is a registered trademark of Advanced Micro Device, Inc. in the United States and other countries.

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 registered 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.

OpenSSL is a registered trademark of OpenSSL Software Foundation in the United States and other countries.

Python is a registered trademark of Python Software Foundation.

RSA and RC4 are registered trademarks of EMC Corporation in the United States and other countries.

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

ssh is a registered trademark of SSH Communications Security, Inc.

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

Windows is a registered trademark or 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 device, 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.

■ **Note**

Information in this document is subject to change without notice.

■ **Editions history**

December 2023 (Edition 1) AX38S-S013X-C0

■ **Copyright**

Preface

■ Applicable products and software versions

This manual applies to the models in the AX3660S series of switches. It also describes the function of OS-L3M version 12.1 of the software. The described function is that supported by the software licenses and by optional licenses.

Before you operate the Switch, 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 the functions common to both the SL-L3A and SL-L3L software licenses. Functions that are not common are indicated as follows.

[SL-L3A]:

The description applies to the SL-L3A software 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:

https://www.alaxala.com/en/
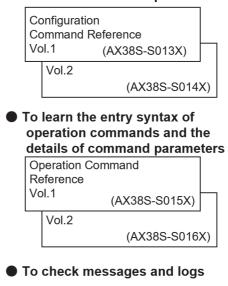
■ Reading sequence of the manuals

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.

● **To learn how to unpack the switch and the basic settings for initial installation**

Quick Start Guide

(AX36S-Q002X)

● **To check the hardware equipment conditions and how to handle the hardware**

Hardware Instruction Manual

(AX36S-H002X)

Transceiver
Hardware Instruction Manual

(AX-COM-H001X)

● **To learn the software functions, configuration settings, and use of operation commands**

Configuration Guide
Vol.1
(AX38S-S010X)

Vol.2
(AX38S-S011X)

Vol.3
(AX38S-S012X)

● **To learn the entry syntax of configuration commands and the details of command parameters**

Configuration
Command Reference
Vol.1 (AX38S-S013X)

Vol.2
(AX38S-S014X)

● **To learn the entry syntax of operation commands and the details of command parameters**

Operation Command
Reference
Vol.1
(AX38S-S015X)

Vol.2
(AX38S-S016X)

● **To check messages and logs**

Message Log Reference

(AX38S-S017X)

● **To learn how to troubleshoot a problem**

Troubleshooting Guide

(AX36S-T002X)

■ Conventions: The terms "Switch" and "switch"

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

● AX3660S 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
AES	Advanced Encryption Standard
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
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
CA	Certificate Authority
CBC	Cipher Block Chaining
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
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
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
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair 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
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
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
PGP	Pretty Good Privacy
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
PMTU	Path Maximum Transmission Unit
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PTP	Precision Time Protocol

QoS	Quality of Service
QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
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
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
Sync-E	Synchronous Ethernet
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLS	Transport Layer Security
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
VLAN	Virtual LAN
VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web

■ Conventions: KB, MB, GB, and TB

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

Contents

14.   Advanced Script   245

PART 3: Network Interfaces

15.   Ethernet   265

PART 4: Layer 2 Switching

19.   VXLAN   375

20.   Spanning Tree Protocols   391

21.   Ring Protocol   459

PART 5: Filters and QoS

PART 7: Security

31.   DHCP snooping   825

PART 8: High Reliability Based on Redundant Configurations

32.   GSRP   851

PART 9: Network Monitoring Function

PART 11: Configuration Error Messages

1 Reading the Manual

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 device.

Notes

Provides cautionary information on using the command.

Related commands

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

Command mode list

The following table lists the command modes.

Table 1-1: List of configuration commands

No.	Prompt displayed for the command mode	Description of command mode	Mode transition command
1	(config)	Global configuration mode	# enable # configure
2	(config-line)	Configuring remote login and console settings	(config)# line vty (config)# line console
3	(config-if)	Configuring the management port	(config)# interface mgmt
		Configuring an Ethernet interface	(config)# interface gigabitethernet (config)# interface tengigabitethernet (config)# interface fortygigabitethernet (config)# interface hundredgigabitethernet
		Configuring a port channel interface	(config)# interface port-channel
		Configuring a VLAN interface	(config)# interface vlan
		Configuring a VXLAN interface [SL-L3A]	(config)# interface vxlan
		Configuring a loopback interface	(config)# interface loopback
		Configuring the null interface	(config)# interface null
4	(config-if-range)	Configuring multiple Ethernet interfaces	(config)# interface range gigabitethernet (config)# interface range tengigabitethernet (config)# interface range fortygigabitethernet (config)# interface range hundredgigabitethernet
		Configuring multiple port channel interfaces	(config)# interface range port-channel
		Configuring multiple VLAN interfaces	(config)# interface range vlan
5	(config-subif)	Configuring an Ethernet subinterface [SL-L3A]	(config)# interface gigabitethernet (config)# interface tengigabitethernet (config)# interface fortygigabitethernet (config)# interface hundredgigabitethernet (When the subinterface index is specified)
		Configuring a port channel subinterface [SL-L3A]	(config)# interface port-channel (When the subinterface index is specified)
6	(config-vlan)	Configuring a VLAN	(config)# vlan

No.	Prompt displayed for the command mode	Description of command mode	Mode transition command
7	(config-mst)	Configuring Multiple Spanning Tree	(config)# spanning-tree mst configuration
8	(config-axrp)	Configuring the Ring Protocol	(config)# axrp
9	(config-gsrp)	Configuring GSRP	(config)# gsrp
10	(config-ext-nacl)	Configuring an IPv4 packet filter	(config)# ip access-list extended
11	(config-std-nacl)	Configuring an IPv4 address filter	(config)# ip access-list standard
12	(config-ipv6-acl)	Configuring an IPv6 filter	(config)# ipv6 access-list
13	(config-ext-macl)	Configuring a MAC filter	(config)# mac access-list extended
14	(config-ip-qos)	Configuring IPv4 QoS	(config)# ip qos-flow-list
15	(config-ipv6-qos)	Configuring IPv6 QoS	(config)# ipv6 qos-flow-list
16	(config-mac-qos)	Configuring MAC QoS	(config)# mac qos-flow-list
17	(dhcp-config)	Configuring DHCP	(config)# ip dhcp pool
18	(config-dhcp)	Configuring IPv6 DHCP (PD)	(config)# ipv6 dhcp pool
19	(config-route-map)	Configuring a route map	(config)# route-map
20	(config-rtr-rip)	Configuring RIPng	(config)# ipv6 router rip
21	(config-router)	Configuring RIP	(config)# router rip
		Configuring OSPF	(config)# router ospf
		Configuring BGP4/BGP4+	(config)# router bgp
22	(config-rtr)	Configuring OSPFv3	(config)# ipv6 router ospf
23	(config-router-af)	Configuring RIP for each VRF	(config)# router rip (config-router)# address-family ipv4 vrf
		Configuring BGP4 for each VRF (config-router-af) (ipv4 vrf) mode	(config)# router bgp (config-router)# address-family ipv4 vrf
		Configuring BGP4+ global network (config-router-af) (ipv6) mode	(config)# router bgp (config-router)# address-family ipv6
		Configuring BGP4+ for each VRF (config-router-af) (ipv6 vrf) mode	(config)# router bgp (config-router)# address-family ipv6 vrf
24	(config-auto-cf)	Configuring auto-config	(config)# auto-config
25	(config-netconf)	Configuring netconf	(config)# netconf
26	(config-view)	Configuring view	(config)# parser view
27	(config-ether-cfm)	Configuring the domain name and MA	(config)# ethernet cfm domain

No.	Prompt displayed for the command mode	Description of command mode	Mode transition command
28	(config-track-object)	Configuring the policy-based routing tracking function	(config)# track-object
29	(config-pol)	Configuring policy-based routing list information	(config)# policy-list
30	(config-dest-mirror)	Configuring mirror ports for policy-based mirroring	(config)# destination-interface-list
31	(config-bfd)	Configuring BFD	(config)# bfd name
32	(config-applet)	Configuring the applet functions	(config)# event manager applet <applet name>

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, Subnet mask	Specify these 4-byte 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
add/remove specification	Add to or delete from the information when multiple items 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 100,200-210 switchport trunk allowed vlan remove 100,200-210 switchport isolation interface add gigabitethernet 1/0/1-3, tengigabitethernet 1/0/25-26 switchport isolation interface remove gigabitethernet 1/0/1-3, tengigabitethernet 1/0/25-26

■ Arbitrary 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

Char-acter	Code	Char-acter	Code	Char-acter	Code	Char-acter	Code	Char-acter	Code	Char-acter	Code
$	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 <switch no.>, <nif no.>, and <port no.> values

The following table lists the range of parameter <switch no.>, <nif no.>, and <port no.> values.

Table 1-5: Range of <switch no.>, <nif no.> and <port no.> values for AX3660S models

Model	Range of values		
	<switch no.>	<nif no.>	<port no.>
AX3660S-24T4X	1 to 2	0	1 to 30
AX3660S-24T4XW			1 to 30
AX3660S-48T4XW			1 to 54
AX3660S-16S4XW			1 to 46
AX3660S-24S8XW			1 to 46
AX3660S-48XT4QW			1 to 52
AX3660S-24X4QW			1 to 52
AX3660S-48X4QW			1 to 52

■ How to specify <interface id list>

For <interface id list>, you can use hyphens (-) and commas (,) to specify the following multiple Ethernet interfaces. You can also specify a single interface by omitting the content enclosed with brackets ([]). The range of permitted values is the same as the range of <switch no.>, <nif no.>, and <port no.> values in the above tables.

- For Gigabit Ethernet interfaces

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

- For 10 Gigabit Ethernet interfaces

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

- For 40 Gigabit Ethernet interfaces

  fortygigabitethernet <switch no.>/<nif no.>/<port no.>[-<port no.>]

- For 100 Gigabit Ethernet interfaces

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

Example of a range specification that uses hyphens (-) and commas (,):

  gigabitethernet 1/0/1-2, gigabitethernet 1/0/5, tengigabitethernet 1/0/25-26

■ Range of <channel group number> values

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

Table 1-6: Range of <channel group number> values

No.	Model	Range of values
1	All models (When a stack configuration is used)	1 to 96
2	All models (When a standalone configuration is used)	1 to 48

■ Range of <subinterface index> values [SL-L3A]

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

■ Range of <vlan id> values

The range of <vlan id> values is 1 to 4094.

■ How to specify <vlan id list>

For <vlan id list>, you can use hyphens (-) and commas (,) to specify multiple VLAN IDs. You can also specify one VLAN ID. The range of values that can be specified 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 hyphens (-) and commas (,):

    1-3,5,10

Example of a specification displayed in multiple lines

    switchport trunk allowed vlan 100,200,300...

    switchport trunk allowed vlan add 400,500...

■ Range of <vni> values [SL-L3A]

The range of <vni> values is 1 to 16777215.

■ How to specify <vni list> [SL-L3A]

For <vni list>, you can use hyphens (-) and commas (,) to specify multiple VNIs. You can also specify one VNI. The range of values that can be specified is the same as the range of <vni> values above. If there are large amounts of information set for <vni list>, the configuration information might be displayed over multiple lines. Conversely, if the information set in <vni list> is reduced by edits made to VNIs using add/remove, multiple lines of configuration information might be consolidated into one line.

Example of a range specification that uses hyphens (-) and commas (,):

    1-3,5,10

Example of a specification displayed in multiple lines

    member vni 100,200,300...

    member vni add 400,500...

■ Range of <vtep id> values [SL-L3A]

The range of <vtep id> values is 1 to 255.

■ Range of <loopback id> values [SL-L3A]

The range of <loopback id> values is 1 to 256.

■ How to specify the interface

The following table lists the specification methods for parameters <interface type> and <interface number> that correspond to interface type groups.

Table 1-7: How to specify an interface

Interface type group	Interface name to be specified in <interface type>	Interface number to be specified in <interface number>
Ethernet interface	gigabitethernet	<switch no.>/<nif no.>/<port no.>
	tengigabitethernet	<switch no.>/<nif no.>/<port no.>
	fortygigabitethernet	<switch no.>/<nif no.>/<port no.>
	hundredgigabitethernet	<switch no.>/<nif no.>/<port no.>
Ethernet subinterface [SL-L3A]	gigabitethernet	<switch no.>/<nif no.>/<port no.>.<subinterface index>
	tengigabitethernet	<switch no.>/<nif no.>/<port no.>.<subinterface index>
	hundredgigabitethernet	<switch no.>/<nif no.>/<port no.>.<subinterface index>
Port channel interface	port-channel	<channel group number>
Port channel subinterface [SL-L3A]	port-channel	<channel group number>.<subinterface index>
VLAN interface	vlan	<vlan id>
VXLAN interface [SL-L3A]	vxlan	<vtep id>
Loopback interface	loopback	0
		<loopback id> [SL-L3A]
Null interface	null	0
Management port	mgmt	0

■ Specification of multiple interfaces

This specification method is used to collectively set the same information for multiple interfaces. You can specify the interface names and interface numbers that correspond to the following interface type groups among the groups listed in "Table 1-7: How to specify an interface".

- Ethernet interface
- Port channel interface
- VLAN interface

When multiple interfaces are to be specified, interfaces included in the same interface type group can be mixed, but interfaces in different interface type groups cannot be mixed.

Syntax

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

You can specify no more than 8 of the input formats, separating each by a comma (,).

Input example

```
interface range gigabitethernet 1/0/1-3
interface range gigabitethernet 1/0/1-3, gigabitethernet 1/0/11-13
interface range vlan 1-100
```

■ Range of <vrf id> values [SL-L3A]

The range of <vrf id> values is 2 to 256.

■ Specifiable values for the message type

The following table lists the values that can be specified for parameters <message type> and <event kind> that specify the message type.

Table 1-8: Specifiable values for the message type

No.	Specifiable value
1	key
2	rsp
3	sky
4	srs
5	err
6	evt
7	aut
8	dsn
9	tro [SL-L3A]
10	rtm
11	mrp
12	mr6
13	bfd

2 Operation Terminal Connection

ftp-server

Permits access from remote operation terminals by using FTP. To permit or deny a remote operation terminal's access to the Switch, enter config-line mode, create a common access list that is used to restrict both Telnet and FTP access, and specify the IPv4 or IPv6 address of the remote operation terminal in the access list.

Syntax

To set information:

> ftp-server
>
> ftp-server vrf {<vrf id> | all}

To delete information:

> no ftp-server
>
> no ftp-server vrf {<vrf id> | all}

Input mode

`(config)`

Parameters

vrf {<vrf id> | all} [SL-L3A]

> <vrf id>
>
>> Accepts access from the specified VRF. The global network is excluded.
>>
>> If you want to specify an individual VRF to permit access to the device, you can set up to four entries per device.
>
> all
>
>> Accepts access from all VRFs including the global network.
>>
>> 1. Default value when this parameter is omitted:
>>
>> Accepts access from the global network.
>>
>> 2. Range of values:
>>
>> For <vrf id>, specify a VRF ID.
>>
>> For details, see "Specifiable values for parameters".

Default behavior

Does not allow remote FTP access.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When config-line mode is used to specify an access list for the Switch, the access list can be used to control (permit or deny) FTP log-in access to the Switch from remote operation terminals whose IPv4 or IPv6 addresses are specified in the access list.

2. If the vrf all parameter is specified, an individual global network or VRF cannot be specified. [SL-L3A]

3. If you specify an individual VRF to permit access to the device, you can specify a total of up to four VRF IDs by using this command and the "transport input" command. [SL-L3A]

Related commands

line vty

ip access-group

ipv6 access-class

transport input

line console

Entering this command changes the mode to config-line mode, in which information about the specified CONSOLE (RS232C) port can be set.

Syntax

To set information:

line console 0

To delete information:

no line console

Input mode

`(config)`

Parameters

None

Default behavior

The console can be connected to a CONSOLE (RS232C) port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

speed

line vty

Permits remote login to the device by using Telnet or SSH. This command is also used to limit the number of remote users that can be simultaneously logged in to the device.

Configuration with this command enables remote login using Telnet or SSH from any remote operation terminal to be accepted. To restrict login from some terminals, see "Configuration Guide Vol. 1, 10.1.7 Configuring the IP address that permits login from a remote operation terminal" to set ip access-group, ipv6 access-class, or transport input.

Syntax

To set information:

    line vty 0 <number>

To delete information:

    no line vty

Input mode

`(config)`

Parameters

<number>

> Sets the number of users who are able to log in simultaneously.

> 1. Default value when this parameter is omitted:

>   This parameter cannot be omitted.

> 2. Range of values:

>   0 to 15 (The number of users who can log in can be set to any value from 1 to 16.)

Default behavior

Does not accept remote login that uses Telnet or SSH.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Configuration with this command enables remote login using Telnet or SSH from any remote operation terminal to be accepted. To restrict login from some terminals, see "Configuration Guide Vol. 1, 10.1.7 Configuring the IP address that permits login from a remote operation terminal" to set ip access-group, ipv6 access-class, or transport input.

2. If you change the maximum number of concurrent users, current user sessions will not be terminated. The change does not close the sessions of users who are currently logged in.

Related commands

transport input

ip access-group

ipv6 access-class

speed

Sets the communication speed of the CONSOLE (RS232C) port. If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out. If the communication speed is changed from a remote operation terminal while user login authentication from CONSOLE (RS232C) is in progress, authentication might fail.

Syntax

To set or change information:

>   speed <number>

To delete information:

>   no speed

Input mode

`(config-line)`

Parameters

<number>

>   Sets the communication speed for CONSOLE (RS232C) in bit/s.
>
>   1. Default value when this parameter is omitted:
>
>   Sets the communication speed of CONSOLE (RS232C) to 9600 bit/s.
>
>   2. Range of values:
>
>   1200, 2400, 4800, 9600, 19200

Default behavior

The communication speed of CONSOLE (RS232C) is 9600 bit/s.

Impact on communication

None

When the change is applied

If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out.

Notes

1. If a user is already logged in from CONSOLE (RS232C) when the setting is changed, the communication speed is changed after the user logs out. If the communication speed is changed from a remote operation terminal while user login authentication from CONSOLE (RS232C) is in progress, authentication might fail.

Related commands

line console

transport input

Restricts access from remote operation terminals based on protocol.

Permits access only with the Telnet or SSH protocol, whichever is specified, and restricts access that uses other protocols.

Syntax

To set or change information:

transport input {telnet | ssh | all | none}

transport input vrf {<vrf id> | all} {telnet | ssh | all | none}

To delete information:

no transport input

no transport input vrf {<vrf id> | all}

Input mode

`(config-line)`

Parameters

vrf {<vrf id> | all} [SL-L3A]

<vrf id>

Accepts access from the specified VRF. The global network is excluded.

If you want to specify an individual VRF to permit access to the device, you can set up to four entries per device.

all

Accepts access from all VRFs including the global network.

1. Default value when this parameter is omitted:

Accepts access from the global network.

2. Range of values:

For <vrf id>, specify a VRF ID.

For details, see "Specifiable values for parameters".

{telnet | ssh | all | none}

telnet

Accepts remote access that uses the Telnet protocol.

ssh

Accepts remote access that uses the SSH protocol.

all

Accepts remote access that uses any protocol.

Does not accept remote access using any protocol.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

Accepts remote access that uses the Telnet or SSH protocol (when ip ssh is set).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When using SSH, set the "ip ssh" command in global configuration mode.

2. To permit or restrict FTP connections, use the "ftp-server" command in global configuration mode.

3. If the vrf all parameter is specified, an individual global network or VRF cannot be specified. [SL-L3A]

4. If you specify an individual VRF to permit access to the device, you can specify a total of up to four VRF IDs by using this command and the "ftp-server" command. [SL-L3A]

Related commands

line vty

ftp-server

ip access-group

ipv6 access-class

ip ssh

3   Configuration Editing and Operation

end

Ends configuration command mode and returns you to administrator mode.

Syntax

end

Input mode

Configuration command mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the "end" command.

Table 3-1: Response messages for the end command

Message	Description
Unsaved changes found! Do you exit "configure" without save ? (y/n):	You are trying to exit configuration command mode without saving the edited configuration in the startup configuration file. Enter "y" to exit configuration command mode. Enter "n" to abort the "end" command. If necessary, execute the "save" command to save the edited configuration in the startup configuration file.

Notes

1. You can use this command to temporarily exit configuration command mode without saving the configuration in the startup configuration file. If you do so, the editing process of the configuration will still be incomplete. Once editing the configuration is completed, execute the "save" command to save it in the startup configuration file.

2. If you execute this command without saving the edited configuration in the startup configuration file, the configuration will differ from the startup configuration file. For this reason, if you enter configuration command mode again and then enter this command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.

3. Do not press the Ctrl + C keys to interrupt processing while this command is being executed. If the processing is interrupted, configuration command mode will not end. Then, executing a configuration command might cause an error with the message: Logical inconsistency occurred. If this message is output, use this command to end configuration command mode.

Related commands

None

quit (exit)

Returns to the previous mode. If you are in global configuration mode, this command ends configuration command mode and returns you to administrator mode. If you are editing data in a level-2 or level-3 detailed configuration command mode, you are returned one level higher.

For details about operations in user mode and administrator mode, see the manual "Operation Command Reference".

Syntax

quit or exit

Input mode

Configuration command mode, user mode, and administrator mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the "quit (exit)" command.

Table 3-2: Response messages for the quit (exit) command

Message	Description
Unsaved changes found! Do you exit "configure" without save ? (y/n):	You are trying to exit configuration command mode without saving the edited configuration in the startup configuration file. Enter "y" to exit configuration command mode. Enter "n" to abort the "quit (exit)" command. If necessary, execute the "save" command to save the edited configuration in the startup configuration file.

Notes

Note the following if you use the "quit (exit)" command in configuration command mode:

1. You can use this command to temporarily exit configuration command mode without saving the configuration in the startup configuration file. If you do so, the editing process of the configuration will still be incomplete. Once editing the configuration is completed, execute the "save" command to save it in the startup configuration file.

2. If you execute this command without saving the edited configuration in the startup configuration file, the configuration will differ from the startup configuration file. For this reason, if you enter configuration command mode again and then enter this command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.

3. Do not press the Ctrl + C keys to interrupt processing while this command is being executed. If the processing is interrupted, configuration command mode will not end. Then, executing a configuration command might cause an error with the message: Logical inconsistency occurred. If this message is output, use the "end" command to end configuration command mode.

Related commands

None

save (write)

Saves the edited configuration to the startup configuration file or to a backup configuration file.

Syntax

save [<file name>] [debug]

write [<file name>] [debug]

Input mode

Configuration command mode

Parameters

<file name>

Specifies the name of the configuration file to be saved. This file will be the backup configuration file.

- Specifying a local configuration file

  Specify the name of the file to be stored in the flash memory of a device.

- Specifying a remotely-stored configuration file

  Specify a remote file name in either of the following URL formats:

  - FTP

    ftp://[<user name>[:<password>]@]<host>[:<port>]/<file path>

  - TFTP

    tftp://<host>[:<port>]/<file path>

1. Default value when this parameter is omitted:

   The startup configuration file (startup-config) is overwritten by the configuration you have been editing.

debug

Displays details on the communication status when a remote file is specified.

If the error "Data transfer failed." occurs while attempting to access a remote file, re-execute the command with the debug parameter specified to display detailed error messages, such as server responses.

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

The following table describes the response messages for the "save" command.

Table 3-3: Response messages for the save command

Message	Description
Configuration file already exist. Configuration file save to <file name>? (y/n):	This message notifies you that the specified file already exists, and asks you to confirm whether you want to execute the "save" command and overwrite it. Enter "y" to execute the command. Enter "n" to cancel this operation.
Configuration file save to <file name>? (y/n):	This message confirms whether you want to execute the "save" command for the specified file. Enter "y" to execute the command. Enter "n" to cancel this operation.

Notes

1. Saving the configuration file does not exit configuration command mode. To finish editing and exit configuration command mode, use the "exit" command or "end" command.

2. If you do not have permission to write the configuration file to the save destination, your edits are not saved to the file. To save edits to a file on a remote server, your remote server access permissions must be changed to allow you to write to the remote server.

3. You can use the "status" command to check if the configuration has been changed but not saved.

4. If there is insufficient free capacity in internal flash memory, changed configurations cannot be saved. Use the "show flash" operation command to check the free capacity in the user area. Saving a new startup configuration file (/config/system.cnf) requires free capacity equivalent to the size of the existing startup configuration file (/config/system.cnf) plus the size of the configuration you are editing. About 2 MB of free capacity is required for a maximum-size configuration file.

Related commands

None

show

Displays the configuration being edited.

Syntax

show [<command> [<parameter>]]

Input mode

Configuration command mode

Parameters

<command>

Specifies a configuration command.

Specifies parameters such as <vlan id> or <access list name> to limit the displayed items.

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If there are many items in the configuration, the command might take time to execute.

2. If the configuration is edited or the "copy" command is executed while this command is being executed, this command might be aborted.

3. When software is updated, the last-modified time displayed on the first line before and after the device is restarted might be slightly inaccurate.

    If you restart the device after software is updated without saving the startup configuration, the time at which the device was restarted is displayed as the last-modified time on the first line.

Related commands

None

status

Shows the status of the configuration being edited.

Syntax

status

Input mode

Configuration command mode

Parameters

None

Displayed information

The following table describes the items displayed for the "status" command.

Table 3-4: Response messages for the status command

Title		Displayed information
File name		The file being edited is displayed. Because only running-config can be edited, running-config is displayed.
Last modified time		The last-modified time and the person who updated the file are displayed. Depending on the edit status, the following information is displayed: The file contains initial installation defaults, and the file has not been changed: Not modified The file has not been edited since the device was started: \<Date> by \<User> (not modified) The file has been edited and changed but not saved using the "save" command: \<Date> by \<User> (not saved) The file has been edited (changed) and changes saved using the "save" command: \<Date> by \<User> (saved)
Buffer	Total	Displays the total amount of storage that is available, including the configuration file that is currently being edited.
	Available	Displays the amount of storage remaining for use by the configuration file that is currently being edited. This unavailable capacity is also displayed as a percentage of the total amount.
	Fragments	The amount of currently-edited configuration file space that is unavailable -- for example, because it is fragmented (items have been deleted, but the area has not been reclaimed) -- is displayed. This unavailable capacity is also displayed as a percentage of the total amount.
Login user		The names of users currently logged in to the device, and their login times are displayed. edit is displayed next to users who are editing the configuration.

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If the remaining capacity becomes very small, it might not be sufficient to execute some configuration commands.

2. Before and after a device is restarted, the last-modified time displayed on the first line might be slightly inaccurate.

Related commands

None

top

Returns you from a level-2 or level-3 configuration command mode to global configuration mode (level 1).

Syntax

top

Input mode

Configuration command mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

None

Related commands

None

4   Stack

stack enable

The Switch works in stack mode.

To enable or delete the command settings, you need to restart the device.

Note that in a model with stack-dedicated ports, when the stack function is enabled with this command, the "interface fortygigabitethernet" command is set to use the ports only as stack ports.

Syntax

To set information:

  stack enable

To delete information:

  no stack enable

Input mode

`(config)`

Parameters

None

Default behavior

The Switch works in standalone mode.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

The new setting values take effect when the Switch is restarted.

Response messages

The following table describes the response messages for the "stack enable" command.

Table 4-1: Response messages for the stack enable command

Message	Description
After this command execute, please save configuration editing now in startup-config, and please reboot a device. Do you wish to continue ? (y/n):	After executing this command, save the edited configuration in the startup configuration file, and then restart the device. Enter "y" to execute the command. Enter "n" to cancel this operation.

Notes

1. When this command is set or deleted, manually save the configuration in the startup configuration file, and then restart the Switch. After this command is set or deleted, no configurations can be edited until the Switch is restarted.

The configuration cannot be edited until the Switch is restarted after this command is entered, so even if you attempt to enter the configuration that includes this command by using a copy and paste operation, you can only enter up to this command.

2. Some functions are not interoperable with a stack. Therefore, when setting this command, you need to delete such non-interoperable functions. For details, see "Configuration Guide Vol. 1, 7.1.3 Supported functions".

3. When this command is set, the configuration below is also set simultaneously. This disables the functions that are not interoperable with the stack function.

- no service ipv6 dhcp

Related commands

switch priority

switch provision

interface fortygigabitethernet

switch priority

When the Switch is running in stack mode, sets the master selection priority of the member switches.

Syntax

To set or change information:

> switch <switch no.> priority <priority>

To delete information:

> no switch <switch no.> priority

Input mode

(config)

Parameters

<switch no.>

> Specifies a switch number.

> > 1. Default value when this parameter is omitted:

> > This parameter cannot be omitted.

> > 2. Range of values:

> > See "Specifiable values for parameters".

<priority>

> Specifies the master selection priority of the member switches.

> The greater the value, the higher the priority.

> > 1. Default value when this parameter is omitted:

> > This parameter cannot be omitted.

> > 2. Range of values:

> > Specify 1 to 31 in decimal.

Default behavior

The Switch serves as a member switch with the master selection priority of 15.

Impact on communication

None

When the change is applied

After the setting value is changed, the setting takes effect at the next selection of the master or backup.

Notes

None

Related commands

stack enable

switch provision

Sets the device model.

When the Switch is running in stack mode, this command sets the Switch model for the member switches other than this member switch. The information of this member switch is automatically set. You cannot set or delete the information of this member switch.

Syntax

To set information:

> switch <switch no.> provision { 3660-24t4x | 3660-24t4xw | 3660-48t4xw | 3660-16s4xw | 3660-24s8xw | 3660-48xt4qw | 3660-24x4qw | 3660-48x4qw }

To delete information:

> no switch <switch no.> provision

Input mode

`(config)`

Parameters

<switch no.>

> Specifies a switch number.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".

{ 3660-24t4x | 3660-24t4xw | 3660-48t4xw | 3660-16s4xw | 3660-24s8xw | 3660-48xt4qw | 3660-24x4qw | 3660-48x4qw }

> 3660-24t4x
>
> > Sets the AX3660S-24T4X model.
>
> 3660-24t4xw
>
> > Sets the AX3660S-24T4XW model.
>
> 3660-48t4xw
>
> > Sets the AX3660S-48T4XW model.
>
> 3660-16s4xw
>
> > Sets the AX3660S-16S4XW model.
>
> 3660-24s8xw
>
> > Sets the AX3660S-24S8XW model.
>
> 3660-48xt4qw
>
> > Sets the AX3660S-48XT4QW model.
>
> 3660-24x4qw
>
> > Sets the AX3660S-24X4QW model.

3660-48x4qw

Sets the AX3660S-48X4QW model.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The Switch works according to the automatically set information.

Impact on communication

None

When the change is applied

The change takes effect immediately after it is made.

Notes

1. Setting this command automatically creates an Ethernet interface. Also, deleting this command automatically deletes the Ethernet interface.

2. If you want to change information other than that of this member switch, delete this information first, and then reset the information.

3. The switch numbers of member switches that have already made up a stack cannot be set or deleted.

Related commands

interface gigabitethernet

interface tengigabitethernet

interface fortygigabitethernet

interface hundredgigabitethernet

stack enable

5   Management Port

description

Sets supplementary information. The set information can be used as a note about the management port. Note that when this command is set, information can be checked by using ifDescr (SNMP MIB).

Syntax

To set or change information:

description \<string>

To delete information:

no description

Input mode

`(config-if)`

Management port

Parameters

\<string>

Sets supplementary information for the management port.

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 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 "■Arbitrary 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

None

duplex

Sets duplex of the management port.

Syntax

To set information:

    duplex {full | auto}

To delete information:

    no duplex

Input mode

`(config-if)`

    Management port

Parameters

{full | auto}

    Sets duplex of the management port.

    full

        Sets the line to full duplex (fixed) mode.

    auto

        Determines the duplex mode by auto-negotiation.

    1. Default value when this parameter is omitted:

       This parameter cannot be omitted.

    2. Range of values:

       None

Default behavior

auto is set for speed and duplex.

Impact on communication

If this command is used to make change to the management port in an up status, the management port goes down once and then goes up again.

Therefore, the following situations occur:

- If any communication is in progress on the management port, the communication is suspended.
- The dynamic ARP and dynamic NDP entries created on the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.

2. If auto-negotiation is not used, you must set duplex to full and speed to 10, 100.

Related commands

speed

interface mgmt

Moves to the management port level.

Syntax

To set information:

interface mgmt 0

To delete information:

no interface mgmt 0

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. The management port cannot be used unless the IP address is set.
2. Even if the management port is set, the maximum number of interfaces for the capacity limit will not decrease by one to be used for the management port.

Related commands

None

ip routing

Performs IPv4 layer 3 forwarding on the management port.

Syntax

To set information:

    ip routing

To delete information:

    no ip routing

Input mode

`(config-if)`

    Management port

Parameters

None

Default behavior

Does not perform IPv4 layer 3 forwarding on the management port.

Impact on communication

If this command is used to make change to the management port in an up status, the management port goes down once and then goes up again.

Therefore, the following situations occur:

- If any communication is in progress on the management port, the communication is suspended.
- The dynamic ARP and dynamic NDP entries created on the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Forwarding a large number of packets on the management port increases the CPU utilization, which might affect other communications and operations.

Related commands

None

ipv6 routing

Performs IPv6 layer 3 forwarding on the management port.

Syntax

To set information:

ipv6 routing

To delete information:

no ipv6 routing

Input mode

`(config-if)`

Management port

Parameters

None

Default behavior

Does not perform IPv6 layer 3 forwarding on the management port.

Impact on communication

If this command is used to make change to the management port in an up status, the management port goes down once and then goes up again.

Therefore, the following situations occur:

- If any communication is in progress on the management port, the communication is suspended.
- The dynamic ARP and dynamic NDP entries created on the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Forwarding a large number of packets on the management port increases the CPU utilization, which might affect other communications and operations.

Related commands

None

shutdown

Places the management port in the shutdown state.

Syntax

To set information:

> shutdown

To delete information:

> no shutdown

Input mode

`(config-if)`

> Management port

Parameters

None

Default behavior

None

Impact on communication

Communication using the management port becomes unavailable.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

None

speed

Sets the line speed of the management port.

Syntax

To set or change information:

    speed {10 | 100 | auto | auto {10 | 100 | 10 100}}

To delete information:

    no speed

Input mode

`(config-if)`

    Management port

Parameters

{10 | 100 | auto | auto {10 | 100 | 10 100}}

    Sets the line speed of the management port.

    10

        Sets the line speed to 10 Mbit/s.

    100

        Sets the line speed to 100 Mbit/s.

    auto

        Sets the line speed to auto-negotiation.

    auto {10 | 100 | 10 100}

        Auto-negotiation is performed at the specified line speed. This setting prevents the line speed from operating at an unexpected speed, so the line usage rate is prevented from increasing. If negotiation at the specified line speed does not succeed, the link status does not transition to link-up status.

    1. Default value when this parameter is omitted:

       This parameter cannot be omitted.

    2. Range of values:

       None

Default behavior

auto is set for speed and duplex.

Impact on communication

If this command is used to make change to the management port in an up status, the management port goes down once and then goes up again.

Therefore, the following situations occur:

- If any communication is in progress on the management port, the communication is suspended.

- The dynamic ARP and dynamic NDP entries created on the management port are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.
2. If auto-negotiation is not used, you must set duplex to full and speed to 10, 100.

Related commands

duplex

6   Login Security and RADIUS/ TACACS+

aaa accounting commands

Logs accounting information when commands are used.

Syntax

To set or change information:

aaa accounting commands { 15 | 0-15 } default { start-stop | stop-only } [broadcast] group tacacs+

To delete information:

no aaa accounting commands

Input mode

`(config)`

Parameters

{ 15 | 0-15 }

Specifies the command level for accounting.

15

Only configuration commands are subject to accounting.

0-15

Both operation commands and configuration commands are subject to accounting.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

{start-stop | stop-only}

Specifies the trigger of accounting for commands.

start-stop

Sends a start instruction before a command is executed and a stop instruction after the command is executed.

stop-only

Sends a stop instruction before a command is executed.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

broadcast

If this parameter is specified, accounting information is sent in turn to all servers (a maximum of four) set by the "tacacs-server host" command, and continues regardless of success or failure in sending information or receiving acknowledgements from any of the servers.

1. Default value when this parameter is omitted:

Accounting information will be repeatedly sent in turn to a maximum of four servers until it is successfully sent to, and acknowledgements are received from, the servers.

group tacacs+

      The TACACS+ server is used as the accounting server.

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

tacacs-server host

aaa accounting exec

Enables accounting of login and logout.

Syntax

To set or change information:

aaa accounting exec default { start-stop | stop-only } [broadcast] { group radius | group tacacs+ }

To delete information:

no aaa accounting exec

Input mode

`(config)`

Parameters

{start-stop | stop-only}

Sets the trigger for accounting.

start-stop

Sends a start instruction at login and a stop instruction at logout.

stop-only

Sends a stop instruction at logout only.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

broadcast

If this parameter is specified, accounting information is sent in turn to all servers (a maximum of four) set by the "radius-server host" or "tacacs-server host" command, and continues regardless of success or failure in sending information or receiving acknowledgements from any of the servers.

1. Default value when this parameter is omitted:

Accounting information will be repeatedly sent in turn to a maximum of four servers until it is successfully sent to, and acknowledgements are received from, the servers.

{group radius | group tacacs+}

Sets the type of an accounting server.

group radius

The RADIUS server is used as the accounting server.

group tacacs+

The TACACS+ server is used as the accounting server.

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

None

Related commands

radius-server host

tacacs-server host

aaa authentication enable

Specifies the authentication method to be used when changing to administrator mode (by the "enable" command). If the first specified authentication method fails, the second specified method is used for authentication. You can change how authentication works when the first method failed by using the "aaa authentication enable end-by-reject" command.

Syntax

To set or change information:

aaa authentication enable default <method> [<method> [<method>]]

To delete information:

no aaa authentication enable

Input mode

`(config)`

Parameters

default <method> [<method> [<method>]]

Specifies the authentication method to be used when changing to administrator mode ("enable" command) for <method>.

Specify any of the parameters below for <method>. You cannot set the same <method> more than once.

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

enable

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the group radius parameter or the group tacacs+ parameter is specified, you cannot switch to administrator mode if communication with a RADIUS/TACACS+ server is impossible or authentication fails. Therefore, we recommend that you specify the enable parameter at the same time.

Related commands

aaa authentication enable attribute-user-per-method

aaa authentication enable end-by-reject

radius-server

tacacs-server

aaa authentication enable attribute-user-per-method

Based on each authentication method, change the user name attribute to be used for authentication when changing to administrator mode ("enable" command) as follows:

- For RADIUS authentication, $enab15$ is sent as the User-Name attribute.
- For TACACS+ authentication, the login user name is sent as the User attribute.

Syntax

To set information:

aaa authentication enable attribute-user-per-method

To delete information:

no aaa authentication enable attribute-user-per-method

Input mode

`(config)`

Parameters

None

Default behavior

"admin" is sent as the User-Name attribute when changing to administrator mode ("enable" command).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Use this command to suit your RADIUS/TACACS+ server.

Related commands

aaa authentication enable

aaa authentication enable end-by-reject

Terminates authentication if an attempt to change to administrator mode (by the "enable" command) is denied. If the authentication fails due to an abnormality, such as an inability to communicate, the next authentication method specified by the "aaa authentication enable" command is used to perform authentication.

Syntax

To set information:

aaa authentication enable end-by-reject

To delete information:

no aaa authentication enable end-by-reject

Input mode

`(config)`

Parameters

None

Default behavior

If authentication fails, regardless of the reason for failure, the next authentication method specified by the "aaa authentication enable" command is used to perform authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is only valid for authentication methods specified by the "aaa authentication enable" command.

Related commands

aaa authentication enable

aaa authentication login

Specifies the authentication method to be used at login. If the first specified authentication method fails, the second specified method is used for authentication. You can change how authentication works when the first method failed by using the "aaa authentication login end-by-reject" command.

Syntax

To set or change information:

aaa authentication login default <method> [<method> [<method>]]

To delete information:

no aaa authentication login

Input mode

`(config)`

Parameters

default <method> [<method> [<method>]]

Specifies the authentication method to be used at login for <method>.

Specify any of the parameters below for <method>. You cannot set the same <method> more than once.

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

local

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the group radius parameter or the group tacacs+ parameter is specified, you cannot log in to the Switch if communication with a RADIUS/TACACS+ server is impossible or authentication fails. Therefore, we recommend that you specify the local parameter at the same time.

Related commands

radius-server host

tacacs-server host

aaa authentication login console

aaa authentication login end-by-reject

aaa authentication login console

Applies the authentication method specified by the "aaa authentication login" command when the user logs in from the console (RS232C).

Syntax

To set information:

    aaa authentication login console

To delete information:

    no aaa authentication login console

Input mode

`(config)`

Parameters

None

Default behavior

Local password authentication is used when a user logs in from the console (RS232C).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To perform RADIUS/TACACS+ authentication, you must set the "aaa authentication login" command at the same time.

2. When the local parameter is not specified as the authentication method by the "aaa authentication login" command, and the "aaa authentication login console" command is set, the user cannot log in from the console (RS232C) if communication with a RADIUS/TACACS+ server is impossible or authentication fails, or if the user logs in from the backup switch.

Related commands

aaa authentication login

aaa authentication login end-by-reject

aaa authentication login end-by-reject

Terminates authentication if login authentication is denied. If the authentication fails due to an abnormality, such as an inability to communicate, the next authentication method specified by the "aaa authentication login" command is used to perform authentication.

Syntax

To set information:

aaa authentication login end-by-reject

To delete information:

no aaa authentication login end-by-reject

Input mode

`(config)`

Parameters

None

Default behavior

If authentication fails, regardless of the reason for failure, the next authentication method specified by the "aaa authentication login" command is used to perform authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is only valid for authentication methods specified by the "aaa authentication login" command.

Related commands

aaa authentication login

aaa authorization commands

This command is specified to perform command authorization by using a RADIUS server, TACACS+ server, or by using local (configuration-based) authorization.

Note that, after successful login, you will not be authorized to execute any commands except "logout", "exit", "quit", "disable", "end", "set terminal", "show whoami", and "who am i" if any of the following applies:

- If the command class or the command list cannot be obtained as a vendor-specific attribute or an attribute value when authentication is performed on a RADIUS server or a TACACS+ server
- If the user name and the associated command class (username view-class) or command lists (username view, parser view, or commands exec) are not configured when authentication is performed using a local password

Syntax

To set or change information:

aaa authorization commands default <method> [<method> [<method>]]

To delete information:

no aaa authorization commands

Input mode

`(config)`

Parameters

default <method> [<method> [<method>]]

For <method>, specifies the method to be used for command authorization.

Specify any of the parameters below for <method>. You cannot set the same <method> more than once.

group radius

Command authorization is performed by a RADIUS server.

group tacacs+

Command authorization is performed by a TACACS+ server.

local

Local command authorization is performed.

Default behavior

Command authorization is not performed.

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. With this setting, the command class or command list is obtained simultaneously when command authorization is performed on the RADIUS server or TACACS+ server or by using a local password, as specified by the "aaa authentication login" command. The "aaa authorization commands" command alone is not sufficient for command authorization. You also need to have used the "aaa authentication login" command in advance.

2. After successful login, you will not be authorized to execute any commands except "logout", "exit", "quit", "disable", "end", "set terminal", "show whoami", and "who am i" if any of the following applies:

   - If the command class or the command list cannot be obtained as a vendor-specific attribute or an attribute value when authentication is performed on a RADIUS server or a TACACS+ server

   - If the user name and the associated command class (username view-class) or command list (username view) are not configured when authentication is performed using a local password

Related commands

radius-server host

tacacs-server host

aaa authentication login

aaa authorization commands console

parser view

commands exec

username

aaa authorization commands console

Applies the command authorization specified by the "aaa authorization commands" command when the user logs in from the console (RS232C).

Syntax

To set information:

aaa authorization commands console

To delete information:

no aaa authorization commands console

Input mode

`(config)`

Parameters

None

Default behavior

Command authorization is not required when a user logs in from the console (RS232C).

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. The "aaa authorization commands console" command alone is not sufficient for command authorization. You also need to set the "aaa authorization commands" command.

2. With this setting, if a user logs in from the console (RS232C), command authorization is used to restrict the commands that can be executed.

Related commands

aaa authorization commands

banner

Sets the messages to be displayed before and after a user logs in. Depending on the specified parameters, messages can be displayed before or after a user login via the console, Telnet, FTP, or SSH. A separate message can be set for FTP access.

The following table describes how the login message is displayed according to parameter settings.

Table 6-1: List of pre-login messages to be displayed according to settings

Description		Pre-login message to be displayed			
login	login-ftp	Console, Telnet	ftp	SSHv1	SSHv2
Message A is set.	None	Message A is displayed.	Message A is displayed.	Not displayed.	Message A is displayed.
Message A is set.	The disable parameter is set.	Message A is displayed.	Not displayed.	Not displayed.	Message A is displayed.
Message A is set.	Message B is set.	Message A is displayed.	Message B is displayed.	Not displayed.	Message A is displayed.
None	Message B is set.	Not displayed.	Message B is displayed.	Not displayed.	Not displayed.

Table 6-2: List of post-login messages to be displayed according to settings

Description		Post-login message to be displayed			
motd	motd-ftp	Console, Telnet	ftp	Secure remote login (Common to SSHv1 and SSHv2)	SCP, SFTP, Secure command execution (Common to SSHv1 and SSHv2)
Message A is set.	None	Message A is displayed.	Message A is displayed.	Message A is displayed.	Not displayed.
Message A is set.	The disable parameter is set.	Message A is displayed.	Not displayed.	Message A is displayed.	Not displayed.
Message A is set.	Message B is set.	Message A is displayed.	Message B is displayed.	Message A is displayed.	Not displayed.
None	Message B is set.	Not displayed.	Message B is displayed.	Not displayed.	Not displayed.

Syntax

To set or change information:

banner login { {encode "<encoded message>"} | plain-text }

banner login-ftp { {encode "<encoded message>"} | plain-text | disable }

banner motd { {encode "<encoded message>"} | plain-text }

banner motd-ftp { {encode "<encoded message>"} | plain-text | disable }

To delete information:

no banner [{motd | motd-ftp | login | login-ftp }]

Input mode

```
(config)
```

Parameters

login

Sets the message to be displayed before a user logs in via the console, Telnet, FTP, or SSH.

plain-text

Enter the login message as a plain-text string. After the command is entered, the following message appears and you can enter a string in lines.

```
--- Press CTRL+D or only '.' on last line ---
```

At this point, enter the string you want to display for the login message. At the end of the string, press the Ctrl + D keys or enter a period (.) to close the input page.

Entries are automatically set in the encode parameter configuration. Any login message that was set previously is deleted. If, after inputting the login message, you want to check an image of how the login screen will look in text format, use the "show banner {motd | motd-ftp | login | login-ftp } plain-text" command to do so.

1. Default value when this parameter is omitted:

   No login messages are displayed.

2. Range of values:

   A string consisting of a maximum of 720 alphanumeric characters

3. Note on using this parameter:

   When entering login messages, check the screen settings for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the "show banner {motd | motd-ftp | login | login-ftp } plain-text" command is executed or a client is connected, the prompt might be garbled and the screen display might freeze. If you want to cancel login message setting while entering the login message, press the Ctrl+C keys to abort this. If you enter far more characters than the maximum number of characters permitted in a line, you may find that no further keyboard input (including the Ctrl+D keys or a line break) is accepted. If this happens, use the Backspace key to delete entered characters and then re-enter them, or use the Ctrl+C keys to abort.

   While entering a message, if you find that the previous character in a single line is not deleted when you press the Backspace key, change the setting of the Backspace key of the terminal so that the BS control code (ASCII 0x08 ^H) is sent. Note that the Backspace key does not affect characters in other than the current line.

encode "<encoded message>"

Enter a Base64-encoded string as a login message. Any login message that was set previously is deleted. Normally this is used to encode a message that was entered with the plain-text parameter. If you want to check a text-format image of what the login screen message will look like, use the "show banner {motd | motd-ftp | login | login-ftp } plain-text" command.

1. Default value when this parameter is omitted:

   No login messages are displayed.

2. Range of values:

   Enter a Base64-encoded string enclosed in double-quotation marks (") (a maximum of 960 characters).

3. Note on using this parameter:

When entering login messages, check the screen settings for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the "show banner {motd | motd-ftp | login | login-ftp } plain-text" command is executed or a client is connected, the prompt might be garbled and the screen display might freeze.

login-ftp

Individually sets or disables the message to be displayed before a user logs in through FTP access. For FTP access, this setting has priority over the login setting.

plain-text

Enter the login message as a plain-text string. For details, see the plain-text section under the login parameter above.

encode "<encoded message>"

Enter a Base64-encoded string as a login message. For details, see the encode section under the login parameter above.

disable

Does not display a login message for FTP access even when the login parameter is set.

motd

Sets the message to be displayed after a user logs in through Telnet, console, or FTP access.

plain-text

Enter the login message as a plain-text string. For details, see the plain-text section under the login parameter above.

encode "<encoded message>"

Enter a Base64-encoded string as a login message. For details, see the encode section under the login parameter above.

motd-ftp

Individually sets or disables a message to be displayed after a user logs in through FTP access. For FTP access, this setting has priority over the motd setting.

plain-text

Enter the login message as a plain-text string. For details, see the plain-text section under the login parameter above.

encode "<encoded message>"

Enter a Base64-encoded string as a login message.

For details, see the encode section under the login parameter above.

disable

Does not display a login message for FTP access even when the motd parameter is set.

Default behavior

No login messages are displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting a login message, if a client log-in prompt is unnecessary (for example: when no password is required, and the user name is automatically passed by the client), the login message and the post-authentication screen are displayed in turn.

   When entering a login message, check the screen setting for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the "show banner {motd | motd-ftp | login | login-ftp } plain-text" command is executed or a client is connected, the prompt might be garbled and the screen display might freeze.

Related commands

None

commands exec

Adds a command string to a command list used when local command authorization is enabled.

A maximum of 40 commands, including permitted and restricted commands, can be set in a command list.

Syntax

To set information:

commands exec {include | exclude} all <command>

To delete information:

no commands exec {include | exclude} all <command>

Input mode

`(config-view)`

Parameters

{include | exclude}

Restricts use of the specified command string.

Command strings for which the include parameter is specified are configured as permitted commands. Command strings for which the exclude parameter is specified are configured as rejected commands.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

all <command>

Specifies a command string to be added to the command list.

The Switch judges whether the initial character string of the command entered by the user matches any of the command strings specified in the command lists (match beginning).

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 50 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 "■Arbitrary character string" in "Specifiable values for parameters".

In addition, commas (,) cannot be used in this parameter.

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. A maximum of 40 commands, including permitted and restricted commands, can be set in a command list. A string consisting of a maximum of 50 characters can be set as a command string.

Related commands

aaa authorization commands

username

ip access-group

Sets an access list that specifies the IPv4 addresses of remote operation terminals for which remote login to the Switch is permitted or denied. This setting is common to all types of remote access (Telnet, FTP, or SSH).

No more than 128 entries, spread over multiple lines, including access list entries set by using ip access-group and ipv6 access-class, can be set.

Syntax

To set information:

> ip access-group {<access list number>|<access list name>} [vrf {<vrf id>| all}] in

To delete information:

> no ip access-group {<access list number>|<access list name>} [vrf {<vrf id>| all}]

Input mode

`(config-line)`

Parameters

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

> Specifies the ID for an IPv4 address filter access list (an ID for ip access-list standard or an IPv4 address filter specific access list ID for an access-list).

> 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".

vrf {<vrf id> | all} [SL-L3A]

> Applies an access list for access from VRFs.

> <vrf id>

> Applies an access list for access from a specified VRF.

> all

> Applies an access list for access from all VRFs including the global network.

> 1. Default value when this parameter is omitted:

> Applies an access list for access from the global network.

> 2. Range of values:

> For <vrf id>, specify a VRF ID.

> For details, see "Specifiable values for parameters".

Default behavior

Access, using IPv4 addresses, is permitted from all remote operation terminals.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet, FTP, or SSH).

2. To permit FTP connections, set ftp-server.

3. To permit SSH connections, set ip ssh.

4. When ip access-group is not set, access using IPv4 addresses is permitted from all remote operation terminals.

5. Note that changing the registered IP addresses does not close the sessions of users who have already logged in. The change does not close the sessions of users who are currently logged in.

6. The access list that is specified for vrf all is applied after the access lists that are set for the global network and each vrf <vrf id> are applied. [SL-L3A]

Related commands

line vty

ftp-server

ip ssh

transport input

ipv6 access-class

access-list

ip access-list standard

ipv6 access-class

Sets an access list that specifies the IPv6 addresses of remote operation terminals for which remote login to the Switch is permitted or denied. This setting is common to all types of remote access (Telnet, FTP, or SSH).

No more than 128 entries, spread over multiple lines, including access list entries set by using ip access-group and ipv6 access-class, can be set.

Syntax

To set information:

ipv6 access-class <access list name> [vrf {<vrf id>| all}] in

To delete information:

no ipv6 access-class <access list name> [vrf {<vrf id>| all}]

Input mode

`(config-line)`

Parameters

<access list name>

Specifies an IPv6 filter access-list ID (identifier for ipv6 access-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".

vrf {<vrf id> | all} [SL-L3A]

Applies an access list for access from VRFs.

<vrf id>

Applies an access list for access from a specified VRF.

all

Applies an access list for access from all VRFs including the global network.

1. Default value when this parameter is omitted:

Applies an access list for access from the global network.

2. Range of values:

For <vrf id>, specify a VRF ID.

For details, see "Specifiable values for parameters".

Default behavior

Access, using IPv6 addresses, is permitted from all remote operation terminals.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet, FTP, or SSH).
2. To permit FTP connections, set ftp-server.
3. To permit SSH connections, set ip ssh.
4. When ipv6 access-class is not set, access using IPv6 addresses is permitted from all remote operation terminals.
5. Note that changing the registered IP addresses does not close the sessions of users who have already logged in. The change does not close the sessions of users who are currently logged in.
6. The access list that is specified for vrf all is applied after the access lists that are set for the global network and each vrf <vrf id> are applied. [SL-L3A]

Related commands

line vty

ftp-server

ip ssh

transport input

ip access-group

ipv6 access-list

parser view

Generates a command list used when local command authorization is enabled. Entering this command switches to config-view mode in which information about the command list can be set.

A maximum of 20 command lists can be generated per device.

Syntax

To set information:

    parser view <view name>

To delete information:

    no parser view <view name>

Input mode

`(config)`

Parameters

<view name>

    Specifies the name of a command list to be generated.

      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.

      An alphabetical character can be specified for the first character of such name, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be specified for the subsequent characters.

      For details, see "Name" in the Parameter type column of the table, "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

    1. A maximum of 20 command lists can be generated per device.

Related commands

aaa authorization commands

commands exec

username

radius-server host

Configures the RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

> radius-server host {<ipv4 address> | <ipv6 address> [interface vlan <vlan id>] | <host name>} [auth-port <port>] [acct-port <port>] [timeout <seconds>] [retransmit <retries>] [key <string>] [{auth-only | acct-only}]

To delete information:

> no radius-server host {<ipv4 address> | <ipv6 address> [interface vlan <vlan id>] | <host name>}

Input mode

`(config)`

Parameters

{<ipv4 address> | <ipv6 address> [interface vlan <vlan id>] | <host name>}

> <ipv4 address>
>
> > Specifies the IPv4 address of the RADIUS server in dot notation.
>
> <ipv6 address> [interface vlan <vlan id>]
>
> > Specifies the IPv6 address of the RADIUS server in colon notation.
> >
> > Specify the interface parameter only when a link-local address is specified.
> >
> > - interface vlan <vlan id>
> >
> >   For <vlan id>, specify the VLAN ID set by the "interface vlan" command.
>
> <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.
> >
> >   When an IPv6 link-local address is specified, specify the interface at the same time.

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 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 "■Arbitrary character string" in "Specifiable values for parameters".

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

{auth-only | acct-only}

Restricts use of the specified RADIUS server. It can be used only for the specified purpose. A RADIUS server specified with the auth-only option is used as a server dedicated to authentication. A RADIUS server specified with the acct-only option is used as a server dedicated to accounting.

1. Default value when this parameter is omitted:

The RADIUS server can be used for all purposes (authentication and accounting).

2. Range of values:

None

retransmit <retries>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

The number of times configured by using radius-server retransmit is used. If no period is set, the initial value is 3.

2. Range of values:

0 to 15

timeout <seconds>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

The period configured by using radius-server timeout is used. If no period is set, the initial value is 5.

2. Range of values:

1 to 30

Default behavior

Because the RADIUS server is not configured, no RADIUS communication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of four RADIUS servers can be specified per device.
2. When multiple RADIUS servers are specified, the RADIUS server that is first in the configuration file listing is the first server used for authentication.
3. If the key parameter is omitted and the "radius-server key" command is not set, the RADIUS server is disabled.

Related commands

radius-server key

radius-server retransmit

radius-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

radius-server key

Sets the default RADIUS server key for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

    radius-server key <string>

To delete information:

    no radius-server key

Input mode

`(config)`

Parameters

<string>

    Specifies the RADIUS key used for encryption or for authentication of communication with the RADI-US server. The same RADIUS key must be set for the client and the RADIUS server.

    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 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 "■Arbitrary 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. The key setting for the "radius-server host" command has priority over the setting for the "radius-server key" command.

Related commands

radius-server host

radius-server retransmit

radius-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

radius-server retransmit

Sets the default number of retransmissions to a RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

> radius-server retransmit <retries>

To delete information:

> no radius-server retransmit

Input mode

`(config)`

Parameters

<retries>

> Specifies the number of times an authentication request is resent to the RADIUS server.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   0 to 15

Default behavior

The default value for the number of times an authentication request is retransmitted to a RADIUS server is 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The retransmit setting for the "radius-server host" command has priority over the setting for the "radius-server retransmit" command.

Related commands

radius-server host

radius-server key

radius-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

radius-server timeout

Sets a response timeout value for a RADIUS server used for authentication, authorization, and accounting purposes.

Syntax

To set or change information:

radius-server timeout <seconds>

To delete information:

no radius-server timeout

Input mode

`(config)`

Parameters

<seconds>

Specifies the timeout period in seconds for a response from the RADIUS server.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 30

Default behavior

The default response timeout value for the RADIUS server is 5 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The timeout setting for the "radius-server host" command has priority over the setting for the "radius-server timeout" command.

Related commands

radius-server host

radius-server key

radius-server retransmit

aaa authentication login

aaa authorization commands

aaa accounting exec

tacacs-server host

Configures the TACACS+ server used for authentication or authorization.

Syntax

To set or change information:

> tacacs-server host {<host name> | <ip address>} [key <string>] [port <port>] [timeout <seconds>] [{auth-only | acct-only}]

To delete information:

> no tacacs-server host {<host name> | <ip address>}

Input mode

`(config)`

Parameters

{<host name> | <ip address>}

> Specifies the IPv4 address or the host name of the TACACS+ server.

> 1. Default value when this parameter is omitted:

> This parameter cannot be omitted.

> 2. Range of values:

> An IPv4 address (in dot notation) or a host name can be specified.

> Specify the host name with 64 or fewer characters. For details about the characters that can be specified for the host name, see "Specifiable values for parameters".

key <string>

> Specifies the shared private key used for encryption or authentication of communication with the TACACS+ server. The same shared private key must be set for the client and the TACACS+ server.

> 1. Default value when this parameter is omitted:

> The shared private key configured by using tacacs-server key is used. If the key is not configured, communication with the TACACS+ server is not encrypted.

> 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 "■Arbitrary character string" in "Specifiable values for parameters".

port <port>

> Specifies the TCP port number for TACACS+ server authentication.

> 1. Default value when this parameter is omitted:

> Port number 49 is used.

> 2. Range of values:

> 1 to 65535

timeout <seconds>

> Sets the timeout period (in seconds) for a response from the TACACS+ server.

111

1. Default value when this parameter is omitted:

   The period configured by using tacacs-server timeout is used. If no period is set, the initial value is 5.

2. Range of values:

   1 to 30

{auth-only | acct-only}

Restricts use of the specified TACACS+ server. It can be used only for the specified purpose.

A TACACS+ server specified with the auth-only parameter is used as a server dedicated to authentication. A TACACS+ server specified with the acct-only parameter is used as a server dedicated to accounting.

1. Default value when this parameter is omitted:

   The TACACS+ server can be used for all purposes (authentication and accounting).

2. Range of values:

   None

Default behavior

Because the TACACS+ server is not configured, no TACACS+ communication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of four TACACS+ servers can be specified per device.
2. When multiple TACACS+ servers are specified, the TACACS+ server that is first in the configuration file listing is the first server used for authentication.

Related commands

tacacs-server key

tacacs-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

aaa accounting commands

tacacs-server key

Sets the default shared private key of a TACACS+ server used for authentication or authorization purposes.

Syntax

To set or change information:

    tacacs-server key \<string\>

To delete information:

    no tacacs-server key

Input mode

`(config)`

Parameters

\<string\>

    Specifies the shared private key used for encryption or authentication of communication with the TACACS+ server. The same shared private key must be set for the client and the TACACS+ server.

    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 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 "■Arbitrary 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. The key setting specific to the "tacacs-server host" command has priority over the setting for the "tacacs-server key" command.

Related commands

tacacs-server host

tacacs-server timeout

aaa authentication login

aaa authorization commands

aaa accounting exec

aaa accounting commands

tacacs-server timeout

Sets the default response timeout value for a TACACS+ server used for authentication or authorization purpose.

Syntax

To set or change information:

tacacs-server timeout <seconds>

To delete information:

no tacacs-server timeout

Input mode

`(config)`

Parameters

<seconds>

Specifies the timeout period in seconds for a response from the TACACS+ server.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 30

Default behavior

The default response timeout value for the TACACS+ server is 5 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The timeout setting specific to the "tacacs-server host" command has priority over the setting of the "tacacs-server timeout" command.

Related commands

tacacs-server host

tacacs-server key

aaa authentication login

aaa authorization commands

aaa accounting exec

aaa accounting commands

username

For a specified user, sets the command list or command class permitted by local command authorization. In addition, this command also specifies the auto-logout period for each user, paging, and help message display behavior.

A maximum of 20 users can be specified per device.

Syntax

To set or change information:

> username <user name> exec-timeout <minutes>
>
> username <user name> terminal-pager {enable | disable}
>
> username <user name> terminal-help {all | no-utility}
>
> username <user name> view <view name>
>
> username <user name> view-class {root | allcommand | noconfig | nomanage | noenable}

To delete information:

> no username <user name>
>
> no username <user name> exec-timeout
>
> no username <user name> terminal-pager
>
> no username <user name> terminal-help
>
> no username <user name> view
>
> no username <user name> view-class

Input mode

`(config)`

Parameters

<user name>

> Specifies the user name to be set.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   Specify a string of no more than 16 characters. Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and underscores (_) can be used for the second and subsequent characters.
>
>   For exec-timeout, terminal-pager, or terminal-help, you can specify default_user, and the settings apply to all users. When default_user is specified, the settings apply only to users who are not specified using a specific user name.

exec-timeout <minutes>

> Specifies the auto-logout time (in minutes) of the specified user. If 0 is specified, auto-logout does not apply. This setting is loaded when a user logs in, and has priority over settings configured by using the "set exec-timeout" operation command before the user logs in.
>
> 1. Default value when this parameter is omitted:

60

2. Range of values:

0 to 60

terminal-pager {enable | disable}

Specifies whether to enable paging (messaging) of the specified user. This setting is loaded when a user logs in, and has priority over the settings configured by using the "set terminal pager" operation command before the user logs in.

enable

Paging is performed.

disable

Paging is not performed.

1. Default value when this parameter is omitted:

enable

2. Range of values:

None

terminal-help {all | no-utility}

For the specified user, specifies what type of operation command help messages can be displayed. This setting is loaded when a user logs in, and has priority over the settings configured by using the "set terminal help" operation command before the user logs in.

all

Enables help messages for all permissible operation commands to be displayed.

no-utility

Enables help messages for all permissible operation commands except for utility commands and file operation commands to be displayed.

1. Default value when this parameter is omitted:

all

2. Range of values:

None

view <view name>

Specifies a command list generated by the "parser view" command.

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.

An alphabetical character can be specified for the first character of such name, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be specified for the subsequent characters.

For details, see "Name" in the Parameter type column of the table, "Specifiable values for parameters".

view-class {root | allcommand | noconfig | nomanage | noenable}

Specifies a command class to be assigned to a user.

Specifies any one of root, allcommand, noconfig, nomanage, and noenable command classes that have

been defined in advance on the Switch.

For details, see "Configuration Guide Vol. 1, Table 10-11 Command classes".

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 changed setting takes effect from the next login.

Notes

1. A maximum of 20 users including default_user can be set per device.

2. When default_user is specified, the settings apply only to users who are not specified using a specific user name. For example, when 0 is set as the exec-timeout value for default_user, if the terminal-pager or terminal-help parameter is set for the user name staff, the setting to be applied to user staff is 60, and this is set as the initial value when the exec-timeout parameter is omitted.

3. For users with ("username" command) parameter settings for at least one of exec-timeout, terminal-pager, and terminal-help (which is all users if default_user is set with this command), these ("username" command) parameter settings override settings made by the "set exec-timeout", "set terminal pager", and "set terminal help" operation commands, and the initial default value applies if the parameter was not specified. In this case, the behavior of each command can be changed temporarily just for the current log-in session by using the "set exec-timeout", "set terminal pager", or "set terminal help" operation commands after the user has logged in.

4. If all of the "username" command exec-timeout, terminal-pager, and terminal-help settings for a certain user are deleted by using this command with "no" ("no username"), the parameter values revert to the values set by the "set exec-timeout", "set terminal pager", or "set terminal help" operation commands (or to the default values if they were not set by these commands) -- they revert to the values that they had before the "username" command was used to set them.

Related commands

aaa authorization commands

parser view

commands exec

7 SSH

ip ssh

Runs an SSH server for remote login to the Switch using SSH.

Configuration with this command and the "line vty" command enables remote access using the SSH protocol from any remote operation terminal to be accepted. To restrict access, set ip access-group, ipv6 access-class, or transport input in line vty mode.

Syntax

To set information:

ip ssh

To delete information:

no ip ssh

Input mode

`(config)`

Parameters

None

Default behavior

Because an SSH server is not running, remote login to the Switch using SSH is not possible.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot log in with SSH only by setting this command. It is necessary to set the number of login users with the "line vty" command.

2. Configuration with this command and the "line vty" command enables remote access using the SSH protocol from any remote operation terminal to be accepted. To restrict access, set ip access-group, ipv6 access-class, or transport input in line vty mode.

3. Just because other SSH information commands (such as "ip ssh version") are set, the SSH server will not run unless this command is set, and therefore remote login to the Switch using SSH is not possible.

Related commands

line vty

transport input

ip ssh authentication

Specifies the user authentication method to be permitted by the SSH server of the Switch.

Syntax

To set or change information:

    ip ssh authentication {publickey | password}

To delete information:

    no ip ssh authentication

Input mode

`(config)`

Parameters

{publickey | password}

    Specify publickey to permit only public key authentication.

    Specify password to permit only password authentication.

      1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

      2. Range of values:

        None

Default behavior

Both public key authentication and password authentication are permitted for the authentication method.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

line vty

transport input

ip ssh authkey

Registers the user public key used for public key authentication on the SSH server.

If you register the user public key so that login with public key authentication is possible, register a target user account with the "adduser" operation command before registering the user public key with this command. Note that the number of users for which the public key can be registered is up to 20 per device.

Syntax

To set or change information:

ip ssh authkey <user name> <authentication key name>

{"<public key>" | load-key-file <file name>}

To delete information:

no ip ssh authkey <user name> <authentication key name>

Input mode

`(config)`

Parameters

<user name>

Specifies a user name for registering a public key with the SSH server function.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

User name (No more than 16 characters)

<authentication key name>

Specifies any name for the user public key index.

Up to 10 keys can be registered for each user. Specify the name that do not duplicate one another.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Key name (No more than 14 characters consisting of alphanumeric characters, hyphens (-), and underscores (_))

{"<public key>" | load-key-file <file name>}

Registers the content of the user public key to be used for public key authentication.

"<public key>"

Directly enter the content of the user public key, enclosed in quotation marks ("").

load-key-file <file name>

Specifies a file name for the user public key on the local directory. A path can be specified in the file name.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

If you specify "<public key>", enter the content of the key in one line without line feeds or spaces. Contents after a space are treated as a comment.

Alphanumeric characters and special characters can be entered for comments. For details, see "■Arbitrary character string" in "Specifiable values for parameters". If characters that cannot be used are included in a comment, they are converted to periods (.) when they are read.

If you specify load-key-file <file name>, transfer the user public key to your home directory using SFTP, SCP, or FTP in advance, and then specify the transferred file name. The current directory is the directory after switching to global configuration mode.

Default behavior

Login with public key authentication is not possible.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the user name for which the user public key is set with this command is not registered as an account on the Switch, the user public key will be automatically enabled when a relevant account is newly registered with the "adduser" operation command.

2. Do not create a directory named as ".ssh" under the home directory of each user. In addition, do not transfer, copy, or generate files under the ".ssh" directory.
   The ".ssh" directory is automatically generated and used by the SSH server function of the Switch. If the user puts the file there, the file will be deleted or overwritten.

Related commands

line vty

transport input

ip ssh ciphers

Restricts the encryption method used by the SSHv2 server. Enumerate common key cryptosystems and authenticated encryption methods to be permitted by the SSHv2 server of the Switch.

Syntax

To set or change information:

ip ssh ciphers <encryption algorithm> [<encryption algorithm> [...]]

To delete information:

no ip ssh ciphers

Input mode

`(config)`

Parameters

<encryption algorithm> [<encryption algorithm> [...]]

Specifies common key cryptosystems and authenticated encryption methods. You cannot set the same <encryption algorithm> more than once.

1. Default value when this parameter is omitted:

   At least one of them must be set. Omitted items are not permitted.

2. Range of values:

   The following common key cryptosystem names and authenticated encryption method names can be specified:

   aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, arcfour256, arcfour128, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, 3des, blowfish

Default behavior

The common key cryptosystems and authenticated encryption methods to be permitted by the SSHv2 server are aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, arcfour256, arcfour128, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, 3des, and blowfish.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Regardless of whether or not this command is set, SSHv1 supports both 3des and blowfish (their settings can be entered but are invalid).

Related commands

line vty

transport input

ip ssh key-exchange

Restricts the key exchange method used by the SSHv2 server. Enumerate key exchange methods to be permitted by the SSHv2 server of the Switch.

Syntax

To set or change information:

ip ssh key-exchange <key exchange algorithm> [<key exchange algorithm> [...]]

To delete information:

no ip ssh key-exchange

Input mode

`(config)`

Parameters

<key exchange algorithm> [<key exchange algorithm> [...]]

Specifies key exchange methods. You cannot set the same <key exchange algorithm> more than once.

1. Default value when this parameter is omitted:
   At least one of them must be set. Omitted items are not permitted.

2. Range of values:

   The following key exchange method names can be specified:
   ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1

Default behavior

The key exchange methods to be permitted by the SSHv2 server are ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The setting of this command is invalid in the SSHv1 protocol (the setting can be entered but is invalid).

Related commands

line vty

transport input

ip ssh macs

Restricts the message authentication code method used by the SSHv2 server. Enumerate message authentication code methods to be permitted by the SSHv2 server of the Switch.

Syntax

To set or change information:

  ip ssh macs <mac algorithm> [<mac algorithm> [...]]

To delete information:

  no ip ssh macs

Input mode

`(config)`

Parameters

<mac algorithm> [<mac algorithm> [...]]

  Specifies message authentication code methods. You cannot set the same <mac algorithm> more than once.

  1. Default value when this parameter is omitted:

     At least one of them must be set. Omitted items are not permitted.

  2. Range of values:

     The following message authentication code method names can be specified:

     hmac-sha2-256, hmac-sha2-512, hmac-md5, hmac-md5-96, hmac-sha1, hmac-sha1-96

Default behavior

The message authentication code methods to be permitted by the SSHv2 server are hmac-sha2-256, hmac-sha2-512, hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

  1. The setting of this command is invalid in the SSHv1 protocol (the setting can be entered but is invalid).

Related commands

line vty

transport input

ip ssh version

Restricts the SSH protocol version to be used by the SSH server. If this command is not set, both SSH protocol versions 1 and 2 are permitted for connection.

Syntax

To set or change information:

ip ssh version {1 | 2}

To delete information:

no ip ssh version

Input mode

`(config)`

Parameters

{1 | 2}

Specify 1 to permit only version 1 for connection.

Specify 2 to permit only version 2 for connection.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

Both SSH protocol versions 1 and 2 are permitted for connection.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For security reasons, we recommend using protocol version 2 only.

Related commands

line vty

transport input

8

Time Settings and NTP

clock timezone

Sets the time zone.

The Switch maintains the date and time internally in Coordinated Universal Time (UTC). This clock time-zone setting affects only time set using the "set clock" command, and the time displayed by using an operation command.

Syntax

To set or change information:

clock timezone <zone name> <hours offset> [<minutes offset>]

To delete information:

no clock timezone

Input mode

`(config)`

Parameters

<zone name>

Specifies the name used to identify a time zone.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

A maximum of seven alphanumeric characters

<hours offset>

Specifies the offset from UTC in hours as a decimal integer.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

-12 to -1, 0, and 1 to 12 (hours)

<minutes offset>

Specifies the offset from UTC in minutes as a decimal integer.

1. Default value when this parameter is omitted:

0

2. Range of values:

0 to 59 (minutes)

Default behavior

UTC is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

set clock

show clock

show logging

ntp access-group

Creates an access group whose access to NTP services can be permitted or denied by means of an IPv4 address filter. The maximum number of filter condition entries for an access list that can be set by using this command is shown below.

For OS-L3M (L3 advanced functions) [SL-L3A]

> 522 entries

For OS-L3M (L3 lite functions)

> 50 entries

Syntax

To set information:

> ntp access-group {query-only | serve-only | serve | peer} {<access list number> | <access list name>} [vrf <vrf id>]

To delete information:

> no ntp access-group {query-only | serve-only | serve | peer} [vrf <vrf id>]

Input mode

`(config)`

Parameters

{query-only | serve-only | serve | peer}

> Sets the mode in which an NTP services are used.
>
> query-only
>
> > Only NTP control queries are permitted.
>
> serve-only
>
> > NTP control queries and NTP broadcast messages are not permitted.
>
> serve
>
> > NTP broadcast messages are not permitted.
>
> peer
>
> > All accesses to NTP services are permitted.
>
> 1. Default value when this parameter is omitted:
>
> This parameter cannot be omitted.
>
> 2. Range of values:
>
> None

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

> Specifies the number or the name of an access list that specifies IPv4 addresses which are permitted or denied access to the NTP service.
>
> 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".

vrf <vrf id> [SL-L3A]

Specifies the VRF to which an IPv4 address filter is applied.

1. Default value when this parameter is omitted:

An IPv4 address filter is applied to the global network.

2. Range of values:

For <vrf id>, specify a VRF ID.

For details, see "Specifiable values for parameters".

Default behavior

All accesses to NTP services are permitted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if ntp peer, ntp server, ntp master, or ntp broadcast client is set and an IPv4 address filter is set.

Notes

1. Implicit discard entries are invalid for access lists specified for this command.

2. If at least one access group is created for either a VRF instance or the global network, any accesses with a source IP address that does not match the specified access list are denied. If no access groups are created, all accesses are permitted.

3. When the source IP address matches access lists for multiple access types, access type keywords are applied according to the following priority:

peer -> serve -> serve-only -> query-only

Related commands

ntp peer

ntp server

access-list

ip access-list

ntp authenticate

Enables the NTP authentication function.

Syntax

To set information:

    ntp authenticate

To delete information:

    no ntp authenticate

Input mode

`(config)`

Parameters

None

Default behavior

The NTP authentication function is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if ntp peer, ntp server, ntp master, or ntp broadcast client is set.

Notes

None

Related commands

ntp authentication-key

ntp trusted-key

ntp authentication-key

Sets an authentication key. This command can set a maximum of 10 authentication key entries.

Syntax

To set or change information:

ntp authentication-key <key id> md5 <value>

To delete information:

no ntp authentication-key <key id>

Input mode

`(config)`

Parameters

<key id>

Specifies the key number in decimal.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 65535

md5 <value>

Specifies a value to be assigned to an authentication key.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

A maximum of 30 ASCII characters

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed if ntp peer, ntp server, ntp master, or ntp broadcast client is set.

Notes

1. For some destination devices, the range of available authentication keys might be less than 32 bits. In this case, set the value of a key to use to a value within the valid range of the destination device.

2. Do not specify 65536 or a larger value as the key number.

Related commands

ntp peer

ntp server

ntp master

ntp authenticate

ntp trusted-key

ntp broadcast client

ntp broadcast

Broadcasts NTP packets to each interface and synchronizes other devices with the Switch.

This command can be used together with "ntp peer" and "ntp server" commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

ntp broadcast [version <number>] [key <key id>]

To delete information:

no ntp broadcast

Input mode

(config-if)

VLAN interface

Parameters

version <number>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

Version 4 is specified by default. If you prefer to use the default value, do not set this parameter.

2. Range of values:

1, 2, or 3

key <key id>

Specifies the authentication key for access. Specify key as the number (in decimal) set for authentication-key.

1. Default value when this parameter is omitted:

No authentication keys are specified.

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 if ntp peer, ntp server, ntp master, or ntp broadcast client is set.

137

Notes

1. This function can use IPv4 only.

2. If no IPv4 addresses are set for an interface, no NTP broadcast packets are sent.

3. To change IPv4 address settings of an interface, delete the ntp broadcast setting first.

4. Do not specify 65536 or a larger value as the key number.

Related commands

ntp broadcast client

ntp authentication-key

ntp broadcast client

Specifies the setting for accepting NTP broadcast messages from devices on the connected subnet. This setting enables the Switch to receive NTP broadcast messages from other devices and synchronize its time with that of other devices. When this command is omitted, no NTP broadcast messages are accepted.

Syntax

To set information:

ntp broadcast client

To delete information:

no ntp broadcast client

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

None

Related commands

ntp broadcast

ntp broadcastdelay

Specifies the estimated latency (time delay) between the NTP broadcast server sending time information and the Switch.

Syntax

To set or change information:

> ntp broadcastdelay <micro seconds>

To delete information:

> no ntp broadcastdelay

Input mode

`(config)`

Parameters

<micro seconds>

> Specifies a delay time. The time is set as a decimal integer in microseconds.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 999999

Default behavior

4000 microseconds are set as the delay time of the NTP broadcast server.

Impact on communication

None

When the change is applied

When the "ntp broadcast client" command is set, the change takes effect immediately after the setting value is changed.

Notes

None

Related commands

ntp broadcast client

ntp master

Designates the switch as a local time server. Perform this setting if a reference NTP server cannot be accessed from the network to which the Switch is normally connected.

Syntax

To set or change information:

>ntp master [<stratum>]

To delete information:

>no ntp master

Input mode

`(config)`

Parameters

<stratum>

>Specifies the stratum value in decimal.

>>1. Default value when this parameter is omitted:

>>8

>>2. Range of values:

>>1 to 15

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 you use the Switch as an NTP server, and 10 or more clients are to be synchronized, synchronization might be temporarily disabled. Although the Switch function is not affected even if the number of clients to be synchronized exceeds 10, consider your environment when deciding the number of clients.

2. If 16 or a larger value is set as the stratum value, the Switch assumes that the stratum value is 15.

Related commands

ntp peer

ntp server

ntp peer

Sets NTP server symmetric active/passive mode. In symmetric active/passive mode, the time of the Switch can be synchronized with that of other devices, and vice versa.

This command can be used together with the "ntp broadcast" and "ntp server" commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

> ntp peer [vrf <vrf id>] <ip address> [version <number>] [key <key id>] [prefer]

To delete information:

> no ntp peer [vrf <vrf id>] <ip address>

Input mode

`(config)`

Parameters

vrf <vrf id> [SL-L3A]

> Specifies the VRF of the devices to be the source or targets of the time synchronization.
>
> > 1. Default value when this parameter is omitted:
> >
> > Belongs to the global network.
> >
> > 2. Range of values:
> >
> > For <vrf id>, specify a VRF ID.
> >
> > For details, see "Specifiable values for parameters".

<ip address>

> Specifies the IPv4 address of an NTP time source (time reference) device or an NTP client device.

version <number>

> Specifies the NTP version number.
>
> > 1. Default value when this parameter is omitted:
> >
> > Version 4 is specified by default. If you prefer to use the default value, do not set this parameter.
> >
> > 2. Range of values:
> >
> > 1, 2, or 3

key <key id>

> Specifies the authentication key for access. Specify key as the number (in decimal) set for authentication-key.
>
> > 1. Default value when this parameter is omitted:
> >
> > No authentication keys are specified.
> >
> > 2. Range of values:
> >
> > 1 to 65535

prefer

> When multiple time reference source devices are specified, a device with the prefer parameter specified takes priority.

> 1. Default value when this parameter is omitted:

> No priorities are set.

> 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 there is a 1000 second (about 16 minute) or longer difference between the time of a time reference source (server) device and the time of this (client) Switch, the specified device time is treated as invalid (not reconcilable) and it is not synchronized. If the time of the time-reference synchronization-source device is correct, use the "set clock" operation command to synchronize the time of this Switch to the time of the time-reference synchronization-source device.

2. If the Switch and other devices are configured in symmetric active/passive mode, it might take a very long time to synchronize these devices. If this happens, we recommend that you reduce the number of devices in the configuration.

3. When a device references multiple time-reference synchronization-source devices, if the time of a high-priority synchronization-source device moves outside of the synchronization range (a 1000 second or longer time difference), other synchronization-source devices will be used as the time reference. If this situation is not fixed, synchronization with the other devices might also be lost. You can change the settings to manually disable the synchronization-source designation of the device whose time has moved out of the valid range. Another solution in this case is to manually reset the time of such a device to the correct value, and synchronization will be recovered.

4. If the IP address of the device is configured as that of its loopback interface, use the loopback interface IP address as the source IP address for sending NTP packets. Therefore, if you set the Switch as the synchronization source or destination, specify the loopback interface IP address as the IP address of the Switch. When adding, changing, or deleting the loopback interface IP address, use the "restart ntp" operation command to re-initialize the ntp program.

5. Do not specify 65536 or a larger value as the key number.

Related commands

ntp server

ntp authentication-key

ntp server

Sets client/server mode and specifies client mode for an NTP server. As a result, the time of this Switch is synchronized to that of a time server. The time of this Switch can be synchronized to that of another device, but the time of another device cannot be synchronized to that of this Switch.

This command can be used together with "ntp broadcast" and "ntp peer" commands to specify a maximum of 10 entries in total.

Syntax

To set or change information:

> ntp server [vrf <vrf id>] <ip address> [version <number>] [key <key id>] [prefer]

To delete information:

> no ntp server [vrf <vrf id>] <ip address>

Input mode

`(config)`

Parameters

vrf <vrf id> [SL-L3A]

> Specifies the VRF to which the Switch whose time is to be synchronized belongs.
>
> > 1. Default value when this parameter is omitted:
> >
> > Belongs to the global network.
> >
> > 2. Range of values:
> >
> > For <vrf id>, specify a VRF ID.
> >
> > For details, see "Specifiable values for parameters".

<ip address>

> Specifies the IPv4 address of a device whose time is to be synchronized.

version <number>

> Specifies the NTP version number.
>
> > 1. Default value when this parameter is omitted:
> >
> > Version 4 is specified by default. If you prefer to use the default value, do not set this parameter.
> >
> > 2. Range of values:
> >
> > 1, 2, or 3

key <key id>

> Specifies the authentication key for access. Specify key as the number (in decimal) set for authentication-key.
>
> > 1. Default value when this parameter is omitted:
> >
> > No authentication keys are specified.
> >
> > 2. Range of values:
> >
> > 1 to 65535

prefer

> When multiple time reference source devices are specified, a device with the prefer parameter specified takes priority.
>
> 1. Default value when this parameter is omitted:
>
>   No priorities are set.
>
> 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 there is a 1000 second (about 16 minute) or longer difference between the time of a time reference source (server) device and the time of this (client) Switch, the specified device time is treated as invalid (not reconcilable) and it is not synchronized. If the time of the time-reference synchronization-source device is correct, use the "set clock" operation command to synchronize the time of this Switch to the time of the time-reference synchronization-source device.

2. If the IP address of the device is configured as that of its loopback interface, use the loopback interface IP address as the source IP address for sending NTP packets. Therefore, if you set the Switch as the synchronization source or destination, specify the loopback interface IP address as the IP address of the Switch. When adding, changing, or deleting the loopback interface IP address, use the "restart ntp" operation command to re-initialize the ntp program.

3. Do not specify 65536 or a larger value as the key number.

Related commands

ntp peer

ntp authentication-key

ntp trusted-key

Sets a security key number to perform authentication for security purposes when synchronizing with other devices. By default, the key to be used for authentication is not set. This command can be used to set a maximum of 10 key number entries.

Syntax

To set information:

> ntp trusted-key <key id>

To delete information:

> no ntp trusted-key <key id>

Input mode

`(config)`

Parameters

<key id>

> Specifies the key number to be used for authentication. For this key, the number (in decimal) set by using authentication-key is specified.

> 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

None

When the change is applied

The change is applied immediately after setting values are changed if ntp peer, ntp server, ntp master, or ntp broadcast client is set.

Notes

1. Do not specify 65536 or a larger value as the key number.

Related commands

ntp authenticate

ntp authentication-key

9   Host Names and DNS

ip domain lookup

Enables or disables the DNS resolver function.

Syntax

To set information:
> no ip domain lookup

To delete information:
> ip domain lookup

Input mode

`(config)`

Parameters

None

Default behavior

The DNS resolver function 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

hostname

ip domain name

ip name-server

ping

traceroute

telnet

ip domain name

Sets the domain name to be used by the DNS resolver.

Syntax

To set or change information:

ip domain name <domain name>

To delete information:

no ip domain name

Input mode

`(config)`

Parameters

<domain name>

Sets the domain name for the Switch.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

No more than 63 alphanumeric characters, periods (.), and hyphens (-) can be used.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

If no ip domain lookup is set, the change is applied to operation after ip domain lookup is entered.

Notes

1. Only one domain name can be set for the Switch.

Related commands

hostname

ip name-server

ip domain lookup

ip domain reverse-lookup

Disables or enables the reverse lookup function (function for using an IP address to search for a host name) of the DNS resolver function.

Syntax

To set information:

    no ip domain reverse-lookup

To delete information:

    ip domain reverse-lookup

Input mode

`(config)`

Parameters

None

Default behavior

When the DNS resolver function is enabled, the reverse lookup function is also enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the DNS resolver function is disabled, it will not work regardless of this setting.
2. If the reverse lookup function of the DNS resolver function is disabled by this setting, a host name might not be displayed for the "traceroute" operation command or the "show ntp associations" command.

Related commands

ip domain lookup

ip domain name

ip name-server

traceroute

show ntp association

ip host

Sets host name information mapped to an IPv4 address. This command can configure a maximum of 20 entries.

Syntax

To set or change information:

ip host <name> <ip address>

To delete information:

no ip host <name>

Input mode

`(config)`

Parameters

<name>

Specifies a host name to be assigned to an IPv4 address.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify the host name with 63 or fewer characters. For details about the characters that can be specified, see "Specifiable values for parameters".

<ip address>

Specifies the IPv4 address of a device for which a host name is set in dot notation.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. localhost cannot be set as a host name.

2. 127.*.*.* cannot be set as an IPv4 address.

3. A class D or class E IPv4 address cannot be set.

4. Host names are not case sensitive.

5. If the same host name is specified for the "ip host" command and the "ipv6 host" command, the "ip host" command takes priority.

Related commands

ping

traceroute

telnet

ip name-server

Sets the name server referenced by the DNS resolver. A maximum of three name servers can be specified. If multiple name servers are specified, inquiries to the name servers are performed in the order in which they were set. Because the DNS resolver function is enabled by default, it works as soon as the name server has been set.

Syntax

To set information:

ip name-server <ip address>

To delete information:

no ip name-server <ip address>

Input mode

`(config)`

Parameters

<ip address>

Specifies the IPv4 address of a name server in dot notation.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

If no ip domain lookup is set, the change is applied to operation after ip domain lookup is entered.

Notes

1. Set the IP address (ip name-server) of the DNS server correctly. If the IP address of a DNS server is not set correctly, it might take time until a communication failure with the DNS server is detected when a host name is referenced, and operation might be affected (Example: It takes time until the login prompt appears when a remote connection is established from another device to the Switch via Telnet).

   One way to check the DNS server status is to use the "nslookup" command as shown below.

   `nslookup -retry=1 <host name to be referred> [<IP address of a DNS server>]`

   If the IP address of a DNS server is correct, information about the specified host is displayed as shown below.

   ```
   Server: (Host name of the DNS server)
   Address: (IP address of the DNS server)
   Name: (Specified host name)
   Address: (IP address of the specified host)
   ```

   If the IP address of the DNS server is not correct, the following is displayed:

```
*** Can't find server name for address (IP address of the DNS server): Timed out
```

2. 127.*.*.* cannot be specified as an IP address.

3. Class D and class E addresses cannot be set as IP addresses.

4. AAAA query information cannot be referenced by using IPv6. AAAA query information is referenced by IPv4.

Related commands

ip domain name

ip domain lookup

ipv6 host

Sets host name information mapped to an IPv6 address. This command can configure a maximum of 20 entries.

Syntax

To set or change information:

    ipv6 host <name> <ipv6 address>

To delete information:

    no ipv6 host <name>

Input mode

`(config)`

Parameters

<name>

    Specifies a host name to be assigned to an IPv6 address.

    1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

    2. Range of values:

        Specify the host name with 63 or fewer characters. For details about the characters that can be specified, see "Specifiable values for parameters".

<ipv6 address>

    Specifies the IPv6 address of a device for which a host name is set in colon notation.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. localhost cannot be set as a host name.

2. Host names are not case sensitive.

3. If the same host name is specified for the "ipv6 host" command and the "ip host" command, the "ip host" command takes priority.

Related commands

ping ipv6

traceroute ipv6

telnet

10 Device Management

power redundancy-mode

Configures the output of operation messages according to the power status.

Syntax

To set information:

    power redundancy-mode redundancy-check

To delete information:

    no power redundancy-mode

Input mode

`(config)`

Parameters

redundancy-check

    For the fixed power supply model

        Outputs an operation message with the event level of 8 when the input power is not supplied or when an abnormal voltage is detected.

    For the replaceable power supply model

        Checks if the power is supplied in a redundant configuration.

        If not, an operation message is output to notify of that.

    1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

    2. Range of values:

        None

Default behavior

For the fixed power supply model

    Outputs an operation message with the event level of 4 when the input power is not supplied or when an abnormal voltage is detected.

For the replaceable power supply model

    Does not check if the power is supplied in a redundant configuration.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

swrt_multicast_table

This command is set when the IP multicast routing function and the IGMP or MLD snooping function are used together on the Switch. By setting this command, you can apply information learned from IGMP or MLD snooping when IP multicast forwarding is performed.

You need to restart the device to enable the command settings. Accordingly, you must set this command during the first step of actual operation.

Syntax

To set information:

> swrt_multicast_table

To delete information:

> no swrt_multicast_table

Input mode

`(config)`

Parameters

None

Default behavior

The IP multicast routing function and the IGMP or MLD snooping function cannot be used together on the Switch.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

If you set this command, 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. When you set this command to use the IGMP snooping function, make sure that the IPv4 multicast routing function is used for the target VLANs. The IGMP snooping function is disabled for VLANs if the IPv4 multicast routing function is not used.

2. The following describes functional situations when this command is set to use the MLD snooping function:

   - If a pattern that allocates resources to IPv6 routing is set for the "swrt_table_resource" command, make sure that the IPv6 multicast routing function is used for the target VLANs. The MLD snooping function is disabled for VLANs if the IPv6 multicast routing function is not used.
   - If a pattern that allocates resources only to IPv4 routing is set for the "swrt_table_resource" command, the MLD snooping function is enabled for the target VLANs.

Related commands

None

swrt_table_resource

Sets the allocation pattern for the number of routing table entries for a device. By changing the allocation pattern according to the running mode, you can concentrate resources on the necessary tables.

You need to restart the device to enable the changes in the settings. Accordingly, you must set this command during the first step of actual operation.

Syntax

To set or change information:

    swrt_table_resource { l3switch-1 | l3switch-2 | l3switch-3 | l3switch-4 }

To delete information:

    no swrt_table_resource

Input mode

`(config)`

Parameters

{ l3switch-1 | l3switch-2 | l3switch-3 | l3switch-4 }

l3switch-1

IPv4 mode. This pattern allocates resources to IPv4 routing.

l3switch-2

IPv4/IPv6 mode. This pattern allocates resources to both IPv4 and IPv6 routing.

l3switch-3

IPv6 unicast priority mode. This pattern allocates more resources to IPv6 unicast routing.

l3switch-4

Layer 2 priority mode. This pattern allocates more resources to Layer 2 switching.

For the number of routing table entries for each allocation pattern, see "Configuration Guide Vol. 1, 3. Capacity limit".

1. Default value when this parameter is omitted:

   l3switch-1

2. Range of values:

   None

Default behavior

The pattern "l3switch-1" is used.

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. If you use this parameter, some protocols (functions) have no entries depending on the pattern used (for example, IPv6 for l3switch-1). In this case, communication is not possible, even if such protocols (functions) are configured.

Related commands

None

system fan mode

Sets the operating mode of the fan.

Syntax

To set or change information:

system fan mode <mode>

To delete information:

no system fan mode

Input mode

`(config)`

Parameters

<mode>

Specifies operating mode 1 or 2 for the fan.

1: Low-noise setting

2: Low-temperature setting

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 and 2

Default behavior

1: The low-noise setting is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system interface hundredgigabitethernet

Enables the QSFP28/QSFP+ shared port of the AX3660S-48XT4QW model to function with the line speed of 100 Gbit/s and disables the corresponding interface. For the relationship between the interface number for the port to function with the 100 Gbit/s line speed and the interface number to be disabled, see "Configuration Guide Vol. 1, 14.5 100GBASE-R setting and exclusive change of 100BASE-TX/1000BASE-T/10GBASE-T port".

Syntax

To set information:

system interface hundredgigabitethernet <switch no.>/<nif no.>/<port no.> enable

To delete information:

no system interface hundredgigabitethernet <switch no.>/<nif no.>/<port no.> enable

Input mode

`(config)`

Parameters

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and the port number.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters". However, the setting range of <port no.> is 49 to 52.

enable

Enables the specified interface to function with the 100 Gbit/s line speed.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The line speed of the interface used is set to 40 Gbit/s.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

If you have changed any values, save the configuration and restart the Switch. The new setting values take effect when the Switch is restarted.

Response messages

The following table describes the response messages for the "system interface hundredgigabitethernet" command.

Table 10-1: Response messages for the system interface hundredgigabitethernet command

Message	Description
After this command execute, please save configuration editing now in startup-config, and please reboot a device. Do you wish to continue?(y/n):	After executing this command, save the edited configuration in the startup configuration file, and then restart the device. Enter "y" to execute the command. Enter "n" to cancel this operation.

Notes

1. For a stack configuration, restart all the member switches that configure the stack.

Related commands

None

system l2-table mode

Sets the method for searching a Layer 2 hardware table (MAC address table).

Syntax

To set information:

system l2-table mode <mode>

To delete information:

no system l2-table mode

Input mode

`(config)`

Parameters

<mode>

Selects the method for searching a table used for registration in the hardware table.

1 to 5

Sets the value that specifies the method used to search the Layer 2 hardware table.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 5

Default behavior

1 is set as the method for searching the table.

Impact on communication

If you set a value of 1 to 5 for the parameter, you need to restart the VLAN program to set the table search method for the hardware. Restarting the VLAN program temporarily prevents data from being sent or received.

When the change is applied

The change is applied when the Switch or VLAN program is restarted.

If you have changed any values, save the configuration and restart the Switch or VLAN program. The new setting values take effect when the Switch is restarted.

Notes

None

Related commands

None

system memory-soft-error

Configures the Switch to output an operation message when a soft error occurs in memory inside the switch processor.

Syntax

To set information:

>   system memory-soft-error log

To delete information:

>   no system memory-soft-error log

Input mode

`(config)`

Parameters

log

>   Outputs an operation message when a soft error occurs in memory inside the switch processor.
>
>   1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.

Default behavior

An operation message is not output when a soft error occurs in memory inside the switch processor.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system port-channel load-balance-all-port

In a stack configuration, if the forwarding destination is a link aggregation where multiple member switches are connected, data will be forwarded to a sending port selected from all ports of each of member switches belonging to the link aggregation.

This command is used to set the basic conditions under which the hardware runs. You must restart the device after you change the settings. Accordingly, you must set this command during the first step of actual operation.

Syntax

To set information:

> system port-channel load-balance-all-port

To delete information:

> no system port-channel load-balance-all-port

Input mode

`(config)`

Parameters

None

Default behavior

In a stack configuration, if the forwarding destination is a link aggregation where multiple member switches are connected, data will be forwarded with the priority given to the port of the member switch that received data.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

If you set this command, make sure you save the configuration and restart the Switch. The new setting values do not take effect until the Switch is restarted.

Notes

None

Related commands

None

system recovery

When a failure occurs in a device, no recovery is performed for the failed part, which will remain stopped after the failure occurs. This function covers the send control section.

Syntax

To set information:

    no system recovery

To delete information:

    system recovery

Input mode

`(config)`

Parameters

None

Default behavior

Recovery is performed and failed parts are re-initialized.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system temperature-warning-level

Outputs an operation message when the intake temperature of the device reaches or exceeds the specified temperature.

Syntax

To set information:

system temperature-warning-level <temperature>

To delete information:

no system temperature-warning-level

Input mode

`(config)`

Parameters

Specifies the intake temperature (in Celsius) for the device.

You can specify the temperature in increments of a degree Celsius.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

25 to 50

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

If the intake temperature of the device has already reached or exceeded the specified temperature, an operation message is immediately output.

Related commands

None

11 **Power Saving Functions**

schedule-power-control port-led

Configures LED brightness levels for a Switch during scheduled power saving operation.

Syntax

To set or change information:

  schedule-power-control port-led { enable | economy | disable }

To delete information:

  no schedule-power-control port-led

Input mode

`(config)`

Parameters

{ enable | economy | disable }

  enable

    Enables automatic brightness adjustment for LEDs of the Switch.

    If the "system port-led trigger" command is not set:

      Sets the LED brightness to normal.

    If the "system port-led trigger" command is set:

      Performs the following automatic LED brightness adjustment:

      1. When automatic LED brightness adjustment is performed, the LED switches to normal brightness mode in which the brightness is the same as that of the LED when it turns on and blinks.

      2. 60 seconds after switching to normal brightness mode by automatic brightness adjustment described in 1, the LED switches to power-saving brightness mode in which the brightness is the same as that of the LED when it turns on and blinks.

      3. 10 minutes after switching to power-saving brightness mode described in 2, the LED switches to turn-off mode. If events occur that cause automatic brightness control to be performed, the LED switches to normal brightness mode in which the brightness is the same as that of the LED when it turns on and blinks.

  economy

    Always turns on and blinks the LEDs of the Switch with power-saving brightness.

  disable

    Turns off the LED of the Switch.

  1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

  2. Range of values:

    None

Default behavior

Turns off the LED of the Switch. Automatic brightness adjustment is not performed.

Impact on communication

None

When the change is applied

The change is applied when the command is set.

Notes

1. The PWR LED, ST1, ST2, ACC (memory card access LED), LINK (MNG), and T/R (MNG) are always lit with normal brightness.

2. If automatic LED brightness adjustment is performed for both a normal time range and a scheduled time range, the adjusted state is inherited when the normal time range and the scheduled time range switch.

Related commands

schedule-power-control time-range

schedule-power-control shutdown

Sets a port that is disabled when scheduled power saving function is in use.

Disabling the port turns off the power, reducing the amount of power consumption.

Syntax

To set information:

> schedule-power-control shutdown interface <interface id list>

To change information:

> schedule-power-control shutdown interface {<interface id list> | add <interface id list> | remove <interface id list> }

To delete information:

> no schedule-power-control shutdown interface

Input mode

`(config)`

Parameters

interface <interface id list>

> Specifies the port to be disabled in list format. If you specify <interface id list> to change information, the information is replaced with the contents of the specified list.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".

interface add <interface id list>

> Adds ports to be disabled 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".

interface remove <interface id list>

> Removes ports to be disabled 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".

Default behavior

Ports will not be disabled.

For the port status, see the "show interfaces" command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you want a port to always be disabled regardless of the schedule, you must set both the "shutdown" command and this command.

2. If you use a comma (,) to set shutdown interface for multiple Ethernet interface lists, shutdown interface can be set for a maximum of 24 lists. If the number of lists exceeds 24, an error occurs.

Related commands

schedule-power-control time-range

schedule-power-control time-range

Specifies the execution time of scheduled power saving function.

Syntax

To set or change information:

> schedule-power-control time-range <entry number> {execution time} action {enable | disable}

> Execution time

> • When a date is specified:

> > date start-time <yymmdd> <hhmm> end-time <yymmdd> <hhmm>

> • When a day of the week is specified:

> > weekly start-time {sun | mon | tue | wed | thu | fri | sat} <hhmm> end-time {sun | mon | tue | wed | thu | fri | sat} <hhmm>

> • When daily is specified:

> > everyday start-time <hhmm> end-time <hhmm>

To delete information:

> no schedule-power-control time-range <entry number>

Input mode

`(config)`

Parameters

<entry number>

> Specifies the identifier used to identify the time of execution.

> This identifier is used to reference the time of execution.

> 1. Default value when this parameter is omitted:

> > This parameter cannot be omitted.

> 2. Range of values:

> > 1 to 50

Execution time parameters

{date | weekly | everyday}

> Specifies the type of execution time to be specified.

> date

> > Specify a date.

> weekly

> > Specify a day of the week.

> everyday

> > Specify a daily execution time.

> 1. Default value when this parameter is omitted:

> > This parameter cannot be omitted.

2. Range of values:

None

start-time <yymmdd> <hhmm>

Specifies the start date and time.

yy

Specifies the last two digits of the year in the range from 00 to 38.

For example, 00 means the year 2000.

mm

Specifies the month in the range from 01 to 12.

dd

Specifies the day of the month in the range from 01 to 31.

hh

Specifies the hour (00 to 23).

mm

Specifies the minute (00 to 59).

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a date for <yymmdd>, and a time for <hhmm>. The range of values that can be specified is from 00:00 on January 1, 2000 to 23:58 on January 17, 2038.

end-time <yymmdd> <hhmm>

Specifies the end date and time.

yy

Specifies the last two digits of the year in the range from 00 to 38.

For example, 00 means the year 2000.

mm

Specifies the month in the range from 01 to 12.

dd

Specifies the day of the month in the range from 01 to 31.

hh

Specifies the hour (00 to 23).

mm

Specifies the minute (00 to 59).

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a date for <yymmdd>, and a time for <hhmm>. The range of values that can be specified is from 00:01 on January 1, 2000 to 23:59 on January 17, 2038.

start-time {sun | mon | tue | wed | thu | fri | sat} <hhmm>

Specifies the start day of the week and the time.

sun

> Sets Sunday.

mon

> Sets Monday.

tue

> Sets Tuesday.

wed

> Sets Wednesday.

thu

> Sets Thursday.

fri

> Sets Friday.

sat

> Sets Saturday.

hh

> Specifies the hour (00 to 23).

mm

> Specifies the minute (00 to 59).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Select sun, mon, tue, wed, thu, fri, or sat, and specify a time for <hhmm>.

end-time {sun | mon | tue | wed | thu | fri | sat} <hhmm>

Specifies the end day of the week and the time.

sun

> Sets Sunday.

mon

> Sets Monday.

tue

> Sets Tuesday.

wed

> Sets Wednesday.

thu

> Sets Thursday.

fri

> Sets Friday.

sat

> Sets Saturday.

hh

> Specifies the hour (00 to 23).

mm

Specifies the minute (00 to 59).

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Select sun, mon, tue, wed, thu, fri, or sat, and specify a time for <hhmm>.

start-time <hhmm>

Specifies the start time.

hh

Specifies the hour (00 to 23).

mm

Specifies the minute (00 to 59).

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a time for <hhmm>.

end-time <hhmm>

Specifies the end time.

hh

Specifies the hour (00 to 23).

mm

Specifies the minute (00 to 59).

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a time for <hhmm>.

action {enable | disable}

Specifies the power control behavior for the execution time.

enable

Enables the setting specified by using a configuration command for the scheduled power saving function for the time of execution set by using this command.

disable

Disables the setting specified by using a configuration command for the scheduled power saving function for the time of execution set by using this command. Thereafter, the following configuration command settings are enabled:

• shutdown

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. If the execution time ranges of different action parameters overlap, the action disable setting takes precedence.

2. The following restriction applies when you set the execution time:
   - If date is specified for the type of execution time, the end time must be later than the start time.

Related commands

None

system port-led

Configures the LED brightness of a Switch.

Syntax

To set or change information:

system port-led { enable | economy | disable }

To delete information:

no system port-led

Input mode

`(config)`

Parameters

{ enable | economy | disable }

enable

Enables automatic brightness adjustment for LEDs of the Switch.

If the "system port-led trigger" command is not set:

Sets the LED brightness to normal.

If the "system port-led trigger" command is set:

Performs the following automatic LED brightness adjustment:

1. When automatic LED brightness adjustment is performed, the LED switches to normal brightness mode in which the brightness is the same as that of the LED when it turns on and blinks.

2. 60 seconds after switching to normal brightness mode by automatic brightness adjustment described in 1, the LED switches to power-saving brightness mode in which the brightness is the same as that of the LED when it turns on and blinks.

3. 10 minutes after switching to power-saving brightness mode described in 2, the LED switches to turn-off mode. If events occur that cause automatic brightness control to be performed, the LED switches to normal brightness mode in which the brightness is the same as that of the LED when it turns on and blinks.

economy

Always turns on and blinks the LEDs of the Switch with power-saving brightness.

disable

Turns off the LED of the Switch.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The LEDs of the Switch turn on and blink with normal brightness. Automatic brightness adjustment is not performed.

Impact on communication

None

When the change is applied

The change is applied when the command is set.

Notes

1. The PWR LED, ST1, ST2, ACC (memory card access LED), LINK (MNG), and T/R (MNG) are always lit with normal brightness.

2. During use of the scheduled power saving function, the Switch works according to the configuration of the "schedule-power-control port-led" command.

Related commands

None

system port-led trigger console

Logging in to and logging out of a device via a console connection triggers automatic LED brightness adjustment.

Syntax

To set information:

system port-led trigger console

To delete information:

no system port-led trigger console

Input mode

`(config)`

Parameters

None

Default behavior

Logging in to and logging out of a device via a console connection does not trigger automatic LED brightness adjustment.

Impact on communication

None

When the change is applied

The change is applied when the command is set.

Notes

1. To enable automatic brightness adjustment, specify the enable parameter in the "system port-led" or the "schedule-power-control port-led" command.

Related commands

system port-led

schedule-power-control port-led

system port-led trigger interface

Sets link-up and link-down of the specified port as a trigger for automatic LED brightness adjustment.

Syntax

To set information:

   system port-led trigger interface <interface id list>

To change information:

   system port-led trigger interface {<interface id list> | add <interface id list> | remove <interface id list> }

To delete information:

   no system port-led trigger interface

Input mode

`(config)`

Parameters

<interface id list>

   Specifies ports that trigger automatic LED brightness adjustment. If you specify <interface id list> to change information, the information is replaced with the contents of the specified list.

   1. Default value when this parameter is omitted:

      This parameter cannot be omitted.

   2. Range of values:

      For details about how to specify <interface id list> and the specifiable range of values, see "Specifiable values for parameters".

add <interface id list>

   Adds ports that trigger automatic LED brightness adjustment to the list.

   1. Default value when this parameter is omitted:

      This parameter cannot be omitted.

   2. Range of values:

      For details about how to specify <interface id list> and the specifiable range of values, see "Specifiable values for parameters".

remove <interface id list>

   Removes ports that trigger automatic LED brightness adjustment from the list.

   1. Default value when this parameter is omitted:

      This parameter cannot be omitted.

   2. Range of values:

      For details about how to specify <interface id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

Link-up and link-down of a physical port are not regarded as a trigger for automatic brightness adjustment.

Impact on communication

None

When the change is applied

The change is applied when the command is set.

Notes

1. To enable automatic brightness adjustment, specify the enable parameter in the "system port-led" or the "schedule-power-control port-led" command.

Related commands

system port-led

schedule-power-control port-led

system port-led trigger mc

Insertion and removal of a memory card is regarded as a trigger for automatic LED brightness adjustment.

Syntax

To set information:

system port-led trigger mc

To delete information:

no system port-led trigger mc

Input mode

`(config)`

Parameters

None

Default behavior

Insertion and removal of a memory card is not regarded as a trigger for automatic LED brightness adjustment.

Impact on communication

None

When the change is applied

The change is applied when the command is set.

Notes

1. To enable automatic brightness adjustment, specify the enable parameter in the "system port-led" or the "schedule-power-control port-led" command.

Related commands

system port-led

schedule-power-control port-led

12 Log Data Output Function

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 function 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 message type of log information to be output as an email. Multiple message 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 message type for operation logs to be output.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify the value with 3 characters. For details about the message type that can be entered, see "Specifiable values for parameters".

Default behavior

The behavior is the same as when only evt and err is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The message type set by using this command is applied to all destination email addresses specified by the "logging email" command.

2. If the message type is set by using this command, the default message types (evt and err) become invalid and only the message types that have been set take effect.

Related commands

logging email

logging email-from

Sets the sender of log information to be 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 the "logging email" 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 sending interval for emailing output log information.

Syntax

To set or change information:

    logging email-interval <seconds>

To delete information:

    no logging email-interval

Input mode

`(config)`

Parameters

<seconds>

    Specifies the email sending interval.

      1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

      2. Range of values:

        1 to 3600 (seconds)

Default behavior

The email sending interval 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 email sending interval set by using this command is applied to all destination email addresses specified by the "logging email" 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 the host name with 64 or fewer 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, or 1 to 65535
> >
> > If 0 is specified, the default value when this parameter is omitted is used.

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 function 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 message type of the log information to be sent to the syslog server. Multiple message 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 message type for operation logs to be output.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify the value with 3 characters. For details about the message type that can be entered, see "Specifiable values for parameters".

Default behavior

The behavior is the same as when only evt and err is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The message type set by using this command is applied to all output destinations specified by the "logging host" command.

2. If the message type is set by using this command, the default message types (evt and err) become invalid and only the message 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 the "logging host" 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:

Specify the host name with 64 or fewer 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> [SL-L3A]

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 message type is EVT or ERR, the information after excluding the time, message ID, and additional information is sent.

For details about the format of log information, see "Message Log Reference, 1.2.2 Format of operation logs".

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 function, 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 data output function 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 device 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:

See the table below for the priorities that can be specified. Note that if a level is specified, information is displayed with the keyword.

Table 12-1: 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	Messages that are intended for notification only
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 the "logging host" command.

Related commands

logging host

13 SNMP

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 "■Arbitrary 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 of 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] [start-up_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 threshold check method. 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:

None

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 "■Arbitrary 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:

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 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) for a reason described in 5. above or other reasons (as a guide, it takes time of about half of the interval value).

Related commands

snmp-server host

rmon event

rmon collection history

Configure 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)`

> Ethernet interface

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 "■Arbitrary character string" in "Specifiable values for parameters".

buckets <bucket number>

> Specifies the number of history entries in which statistics 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>, the behavior is the same as if 50 had been specified.

interval <seconds>

Specifies the time interval (in seconds) for collecting statistics. This parameter is equivalent to history-ControlInterval 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.

Related commands

snmp-server community

rmon event

Sets the control information for the 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 SNMP notifications to the community specified for <community>. This parameter is equivalent to eventType defined in RFC 1757.

1. Default value when this parameter is omitted:

SNMP notifications are not sent.

2. Range of values:

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 "■Arbitrary 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 "■Arbitrary 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 "■Arbitrary 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 SNMP notifications 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 SNMP notifications to the SNMP manager, specify the IP address of the destination SNMP manager and "rmon" by using the "snmp-server host" command.

3. An SNMP notification 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 "■Arbitrary character string" in "Specifiable values for parameters".

{ ro | rw }

> For the manager that has the specified IP address belonging to the community with the specified community name, sets a functional mode for the manager to handle MIB-related information. If ro is specified, Get Request and GetNext Request are permitted. If rw is specified, Get Request, GetNext Request, and Set Request are permitted.
>
> 1. Default value when this parameter is omitted:
>
> ro
>
> 2. Range of values:
>
> None

{<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> [SL-L3A]

Permits accesses from the VRF specified in <vrf id>.

1. Default value when this parameter is omitted:

Permits access from the global network.

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 "■Arbitrary 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 device 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 device. 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 "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The SNMP engine ID value set for a device 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 "■Arbitrary 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:

None

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 "■Arbitrary 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 "■Arbitrary 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 "■Arbitrary 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 destination network management device (SNMP manager) to which SNMP notifications 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 notification> [<snmp notification> [...]]]

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> [SL-L3A]

Sends SNMP notifications to the VRF specified for <vrf id> in the "vrf definition" command.

1. Default value when this parameter is omitted:

SNMP notifications are sent 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 SNMP notifications that will be sent to the SNMP manager.

- If traps is specified, traps will be sent. The SNMP manager does not send a response.
- If informs is specified, informs will be sent. 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:

None

<string>

For SNMPv1 and SNMPv2C, this parameter sets the community name 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 "■Arbitrary character string" in "Specifiable values for parameters".

version { 1 | 2c | 3 { noauth | auth | priv }}

Sets the SNMP notification version. If the version is set to SNMPv3, set the security level at the same time.

The following table lists the SNMP notification version to be set when each parameter is specified.

Table 13-1: Correspondence between the parameter value and SNMP notification version

Specified value of this parameter	SNMP notification version	Security level
version 1	SNMPv1	—
version 2c	SNMPv2C	—
version 3 noauth	SNMPv3	Authentication and encryption are not required.
version 3 auth	SNMPv3	Authentication is required, and encryption is not required.
version 3 priv	SNMPv3	Authentication and encryption are both required.

Legend: —: Not applicable

1. Default value when this parameter is omitted:

   version 1

2. Range of values:

   None

<snmp notification> [<snmp notification> [...]]

Specifies SNMP notifications to be sent.

snmp

Sends the following SNMP notifications:

- coldStart
- warmStart
- linkUp
- linkDown
- authenticationFailure

{ ospf_state | ospf_state_private } [SL-L3A]

Sends SNMP notifications for notifying a change in the OSPF status. If ospf_state is specified, standard SNMP notifications that comply with the RFC are sent. However, if the OSPF domain is being partitioned, all domains other than the domain with the smallest domain number will send private SNMP notifications. If ospf_state_private is specified, all OSPF domains will send private SNMP notifications.

The following table lists SNMP notifications to be sent.

Table 13-2: SNMP notifications for each parameter (Notifying the change of the OSPF status)

Parameter	SNMP notifications
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
ospf_state_private	All domains: • axsOspfVirtIfStateChange • axsOspfNbrStateChange • axsOspfVirtNbrStateChange • axsOspfIfStateChange

{ ospf_error | ospf_error_private } [SL-L3A]

Sends SNMP notifications for notifying reception of an OSPF error packet. If ospf_error is specified, standard SNMP notifications that comply with the RFC are sent. However, if the OSPF domain is being partitioned, all domains other than the domain with the smallest domain number will send private SNMP notifications. If ospf_error_private is specified, all OSPF domains will send private SNMP notifications.

The following table lists SNMP notifications to be sent.

Table 13-3: SNMP notifications for each parameter (Notifying reception of an OSPF error packet)

Parameter	SNMP notifications
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

Parameter	SNMP notifications
ospf_error_private	All domains: • axsOspfIfConfigError • axsOspfVirtIfConfigError • axsOspfIfAuthFailure • axsOspfVirtIfAuthFailure

bgp [SL-L3A]

Sends SNMP notifications for BGP4 link establishment and disconnection.

- bgpEstablished
- bgpBackwardTransitions

vrrp

Sends an SNMP notification when the VRRP status is changed.

- vrrpTrapNewMaster
- vrrpTrapAuthFailure
- vrrpTrapProtoError

rmon

Sends an SNMP notification when the value exceeds the upper threshold or drops below the lower threshold of the rmon alarm.

- risingAlarm
- fallingAlarm

oadp

Sends an SNMP notification when information on an OADP adjacent node is updated.

- axsOadpNeighborCashelastChangeTrap

air-fan

Sends an SNMP notification when a fan stops.

- ax3660sAirFanUnitStopTrap

power

Sends an SNMP notification when a failure occurs in a power supply unit.

- ax3660sPowerSupplyFailureTrap

login

Sends an SNMP notifications when a login fails or succeeds or when a logout occurs.

- ax3660sLoginSuccessTrap
- ax3660sLoginFailureTrap
- ax3660sLogoutTrap

memory

Sends an SNMP notification when a memory shortage occurs in the Switch.

- ax3660sMemoryUsageTrap

system-msg

Sends an SNMP notification when an operation message of the message type ERR or EVT is output.

- ax3660sSystemMsgTrap

temperature

Sends an SNMP notification when the temperature status is changed.

- ax3660sTemperatureTrap

gsrp

Sends an SNMP notification when the GSRP status is changed.

- ax3660sGsrpStateTransitionTrap

axrp

Sends an SNMP notification when the ring fault monitoring status is changed.

- ax3660sAxrpStateTransitionTrap
- ax3660sAxrpMultiFaultDetectionStartTrap
- ax3660sAxrpMultiFaultDetectionStateTransitionTrap

frame_error_snd

Sends an SNMP notification when a frame sending error occurs.

- ax3660sFrameErrorSendTrap

frame_error_rcv

Sends an SNMP notification when a frame reception error occurs.

- ax3660sFrameErrorReceiveTrap

storm-control

Sends an SNMP notification when a storm is detected by the storm control function or when a Switch recovers from a storm.

- ax3660sBroadcastStormDetectTrap
- ax3660sMulticastStormDetectTrap
- ax3660sUnicastStormDetectTrap
- ax3660sBroadcastStormPortInactivateTrap
- ax3660sMulticastStormPortInactivateTrap
- ax3660sUnicastStormPortInactivateTrap
- ax3660sBroadcastStormRecoverTrap
- ax3660sMulticastStormRecoverTrap
- ax3660sUnicastStormRecoverTrap

efmoam

Sends an SNMP notification when a unidirectional link failure is detected.

- ax3660sEfmoamUdldPortInactivateTrap
- ax3660sEfmoamLoopDetectPortInactivateTrap

loop-detection

Sends an SNMP notification when a L2 loop is detected.

- ax3660sL2ldLinkDown
- ax3660sL2ldLinkUp
- ax3660sL2ldLoopDetection

cfm

Sends an SNMP notification when a failure is detected by CC.

- dot1agCfmFaultAlarm

switchport-backup

Sends SNMP notifications for uplink redundancy.

- ax3660sUlrChangeSecondary
- ax3660sUlrChangePrimary
- ax3660sUlrActivePortDown

static-route

Sends an SNMP notification when the status of a gateway that uses the dynamic monitoring function for static routing has changed.

- axsStaticGatewayStateChange
- axsStaticIpv6GatewayStateChange

policy-base [SL-L3A]

Sends an SNMP notification when the routing information for policy-based routing has changed.

- axsPolicyBaseRoutingRouteChange

track-object [SL-L3A]

Sends a private SNMP notification when the track status of the tracking function for policy-based routing has changed.

- axsTrackObjectStateUp
- axsTrackObjectStateDown

lldp

Sends an SNMP notification when information on an LLDP adjacent node is updated.

- lldpV2RemTablesChange

flow-rate-alarm

Sends an SNMP notification when the bandwidth status of QoS entries subject to bandwidth non-compliance notifications has changed.

- ax3660sQosFlowListRateAlarmExceedTrap
- ax3660sQosFlowListRateAlarmConformTrap

1. Default value when this parameter is omitted:

   SNMP notifications are not sent for the 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, temperature, gsrp, axrp, frame_error_snd, frame_error_rcv, storm-control, efmoam, loop-detection, cfm, switchport-backup, static-route, policy-base, track-object, lldp, flow-rate-alarm

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 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 "■Arbitrary 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 when to send an SNMP notification.

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 is sent. The following table provides an overview of the triggers that cause the coldStart set by using this parameter to be sent.

Table 13-4: Triggers causing coldStart to be sent for each parameter

Parameter	Triggers causing coldStart to be sent
limited_coldstart_trap	• When a device starts • When changed to the master while running as a stack
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 changed to the master while running as a stack

1. Default value when this parameter is omitted:

limited_coldstart_trap

2. Range of values:

None

link_trap_bind_info {private | standard}

Configures to select the MIB to be added when a link trap (linkDown or linkUp) is sent.

The following table describes the MIBs to be added when a link trap is sent by setting this parameter.

Table 13-5: MIBs to be added when a link trap is sent, for each parameter

Parameter	MIBs to be added when a link trap is sent
private	• (Common to SNMPv1/SNMPv2C) ifIndex, ifDescr, ifType
standard	• (For SNMPv1) ifIndex • (For SNMPv2C) ifIndex, ifAdminStatus, ifOperStatus

1. Default value when this parameter is omitted:

    standard

2. Range of values:

    None

system_msg_trap_level <level>

Sets the event level of operation messages with the message type of ERR or EVT in decimal for sending the operation messages as private SNMP notifications. An SNMP notification is sent when an event with the severity equal to or higher than the setting value of the event level occurs. The following table shows the setting value and its corresponding event level priority.

Table 13-6: Setting value and its target event level severity

Setting value	Target event level severity
9	Fatal failure
8	Severe failure or higher level
5 to 7	Partial SOFTWARE failure or higher level
4	Network failure or higher level
1 to 3	Warning or higher level

1. Default value when this parameter is omitted:

    9

2. Range of values:

    1 to 9

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 sent 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. The target interface is VLAN. If no IPv4 address has been set for the device, 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

None

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 privacy protocol. You can configure the privacy protocol after the authentication protocol has been configured. The following table lists the combinations of the authentication protocols and the privacy protocols.

Table 13-7: Combination of the authentication protocol and the privacy protocol

No.	Authentication protocol	Privacy protocol
1	None	None
2	HMAC-MD5, HMAC-SHA1, HMAC-SHA-256, or HMAC-SHA-512	None
3	HMAC-MD5, HMAC-SHA1, HMAC-SHA-256, or HMAC-SHA-512	CBC-DES or CFB128-AES-128

Syntax

To set or change information:

snmp-server user <user name> <group name> v3 [auth { md5 | sha | sha256 | sha512 } <authentication password> [priv { des | aes128 } <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 "■Arbitrary 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 "■Arbitrary character string" in "Specifiable values for parameters".

v3 [auth { md5 | sha | sha256 | sha512 } <authentication password> [priv { des | aes128 } <privacy password>]]

auth { md5 | sha | sha256 | sha512 } <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.

sha256: HMAC-SHA-256 is used for the authentication protocol.

sha512: HMAC-SHA-512 is used for the authentication protocol.

priv { des | aes128 } <privacy password>

Specifies the privacy protocol and the privacy password.

des: CBS-DES is used for the privacy protocol.

aes128: CFB128-AES-128 is used for the privacy protocol.

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 and subsequent parameter options are omitted, a privacy protocol will not be used.

2. Range of values:

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 "■Arbitrary character string" in "Specifiable values for parameters".

vrf <vrf id> [SL-L3A]

Permits accesses from the VRF specified in <vrf id>.

1. Default value when this parameter is omitted:

Permits access from the global network.

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 13-8: Number of entries for each parameter

No.	Parameter	Maximum number of entries
1	MIB view	50 entries per device
2	Subtree	30 entries per 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 "■Arbitrary 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:

   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. 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

Suppresses the sending of a link trap (linkDown or linkUp), which is an SNMP notification, when the "no snmp trap link-status" command leads to a link-up or link-down failure on a line.

Syntax

To set information:

    no snmp trap link-status

To delete information:

    snmp trap link-status

Input mode

`(config-if)`

    Ethernet interface

Parameters

None

Default behavior

SNMP notifications are 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

14 Advanced Script

aaa authorization commands script

Sets the command authorization behavior when a Python script executes a command.

Syntax

To set or change information:

aaa authorization commands script {username <user name> | bypass}

To delete information:

no aaa authorization commands script

Input mode

`(config)`

Parameters

{username <user name> | bypass}

Sets the command authorization behavior when a Python script executes a command.

username <user name>

Performs command authorization with the authority of the user name specified in this parameter.

bypass

Command authorization is not performed. All commands can be executed.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For <user name>, enclose a character string consisting of no more than 16 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. However, a hyphen (-) cannot be specified as the first character. 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 "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The setting of the "aaa authorization commands" command is used.

- When the "aaa authorization commands" command is not set

  Command authorization is not performed. All commands can be executed.

- When the "aaa authorization commands" command is set

  All commands cannot be executed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The "aaa authorization commands script" command alone is not sufficient for command authorization. You also need to set the "aaa authorization commands" command. Also, command authorization by the RADIUS server is not supported. You need to configure command authorization by a TACACS+ server or locally.

2. When a Python script is started from an operation terminal via console connection (RS232C), the setting of the "aaa authorization commands console" command determines the command authorization behavior.

   - When the "aaa authorization commands console" command is not set

     Command authorization is not performed. All commands can be executed.

   - When the "aaa authorization commands console" command is set

     Command authorization is performed. However, if the bypass parameter is set, command authorization is not performed. All commands can be executed.

3. When command authorization information (command class and command list) cannot be acquired, any commands cannot be executed.

Related commands

aaa authorization commands

aaa authorization commands console

action

Specifies an action (script startup) to be executed when a monitoring event occurs.

Syntax

To set information:

    action <sequence> python <file name> [<args>...]

To delete information:

    no action <sequence>

Input mode

`(config-applet)`

Parameters

<sequence>

Specifies the ascending order in which actions are performed.

Actions are executed one at a time in the specified order, waiting for the completion of the previous action.

1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

2. Range of values:

    1 to 8

python <file name>

Specifies a script file to be started.

The file installed by the "install script" operation command is started.

1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

2. Range of values:

    Specify a string of no more than 99 characters including the extension (either ".py", ".pyc", or ".pyo").
    Characters that can be used are alphanumeric characters, dots (.), hyphens (-), underscores (_), tildes (~), and hats (^).

<args>...

Specifies command line arguments to be given to the script.

1. Default value when this parameter is omitted:

    None

2. Range of values:

    An <args> can be specified with a maximum of 63 characters. Up to 32 <args> can be registered.

    Specifiable characters are alphanumeric characters and special characters. If you specify multiple <args>, specify them separating each with a space. If you use special characters such as a space in an <args>, enclose the string of the <args> in double quotation marks ("). For details, see "■Arbitrary 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 you change the configuration related to a relevant applet while an action is running, the action will be executed until the end, but actions that have not been executed will not be executed.

Related commands

event timer

event sysmsg

priority

disable

disable

Suppresses the target applet function.

Syntax

To set information:

    disable

To delete information:

    no disable

Input mode

`(config-applet)`

Parameters

None

Default behavior

The applet is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a script installed by the "action" command is running when this command is executed, the script will not be forcibly stopped. To stop the script, use the "stop python" operation command.

Related commands

event timer

event sysmsg

priority

action

event manager applet

Creates an applet. Entering this command switches to config-applet mode, in which events to be monitored and actions to be executed can be registered.

Syntax

To set information:

event manager applet <applet name>

To delete information:

no event manager applet <applet name>

Input mode

```
(config)
```

Parameters

<applet name>

Specifies an applet name.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a string of no more than 31 characters. Alphanumeric characters can be used for the first character, and alphanumeric characters, hyphens (-), and underscores (_) can be used for the second and subsequent characters.

Up to 256 applets can be registered.

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 you delete a relevant applet while an action set by the "action" command is running, the action will be executed until the end, but actions that have not been executed will not be executed.

Related commands

event timer

event sysmsg

priority

disable

action

event sysmsg

Monitors operation messages with the specified message type or the specified message text. For operation message with the message type of ERR and EVT, you can also specify the elements that make up operation messages, such as the switch number and event level, to be monitored.

For details about the elements that make up operation messages, see "Message Log Reference, 1.2.2 Format of operation logs".

Syntax

To set or change information:

event sysmsg [message-type <message type>] [switch <switch no.>] [switch-status {master | backup}] [event-level <event level>] [recovery-event-level <event level>] [event-function <event function> [interface-id <interface id>]] [message-id <message id>] [message-text <message text>] [additional-info-upper <upper number>] [additional-info-lower <lower number>]

One of the above monitoring condition parameters must be specified.

To delete information:

no event sysmsg

Input mode

`(config-applet)`

Parameters

message-type <message type>

Specifies the message type.

1. Default value when this parameter is omitted:

   All message types other than key, rsp, sky, and srs are monitored.

2. Range of values:

   Specify the value with 3 characters. For details about the message type that can be entered, see "Specifiable values for parameters". However, key, rsp, sky, or srs cannot be specified.

switch <switch no.>

Specifies the switch number of the member switch where an event occurred.

1. Default value when this parameter is omitted:

   All member switches are monitored.

2. Range of values:

   1 to 2

switch-status {master | backup}

Specifies the switch status of the member switch where an event occurred.

master

Specifies a member switch running as a master or standalone.

backup

Specifies a member switch running as a backup.

253

    1. Default value when this parameter is omitted:

    All member switches are monitored.

    2. Range of values:

    None

event-level <event level>

Specifies the event level (E3 to E9) of operation messages for failures or warnings. Operation messages with the event level specified by this parameter and the recovery-event-level parameter are monitored.

    1. Default value when this parameter is omitted:

    When the recovery-event-level parameter is also omitted, all event levels are monitored. When the recovery-event-level parameter is specified, the specified event level is monitored.

    2. Range of values:

    Specify the value between 3 and 9. Hyphens (-) and commas (,) can be used to specify multiple values.

recovery-event-level <event level>

Specifies the event level (R5 to R8) of operation messages for failure recovery. Operation messages with the event levels specified by this parameter and the event-level parameter are monitored.

    1. Default value when this parameter is omitted:

    When the event-level parameter is also omitted, all event levels are monitored. When the event-level parameter is specified, the specified event level is monitored.

    2. Range of values:

    Specify the value between 5 and 8. Hyphens (-) and commas (,) can be used to specify multiple values.

event-function <event function>

Specifies an event location.

    1. Default value when this parameter is omitted:

    All locations and functions where an event occurred are monitored.

    2. Range of values:

    Specify the value with 15 or fewer characters. For details about event locations that can be entered, see "Message Log Reference, 1.2.5 Event location".

interface-id <interface id>

Specifies the event interface ID in a regular expression. Regular expressions are specified using POSIX 1003.2 Extended Regular Expression with dot (.), hyphen (-), asterisk (*), plus (+), question mark (?), hat (^), dollar ($), opening bracket ([), closing bracket (]), opening parenthesis ((), closing parenthesis ()), pipe (|), and backslash (\) characters.

    1. Default value when this parameter is omitted:

    All interface IDs are monitored.

    2. Range of values:

    Enclose a character string of no more than 32 characters in double quotation marks ("). For details about event interface IDs that can be entered, see "Message Log Reference, 1.2.6 Event interface ID".

message-id <message id>

Specifies the message ID.

    1. Default value when this parameter is omitted:

All message IDs are monitored.

2. Range of values:

Specify a hexadecimal number of 8 digits or less.

message-text <message text>

Specifies a message text in a regular expression. Regular expressions are specified using POSIX 1003.2 Extended Regular Expression with dot (.), hyphen (-), asterisk (*), plus (+), question mark (?), hat (^), dollar ($), opening bracket ([), closing bracket (]), opening parenthesis ((), closing parenthesis ()), pipe (|), and backslash (\) characters.

1. Default value when this parameter is omitted:

All message texts are monitored.

2. Range of values:

Enclose a character string of no more than 128 characters in double quotation marks (").

additional-info-upper <upper number>

Specifies the upper 4 digits of additional information.

1. Default value when this parameter is omitted:

All the upper 4 digits of additional information are monitored.

2. Range of values:

Specify a hexadecimal number of 4 digits or less.

additional-info-lower <lower number>

Specifies the lower 12 digits of additional information.

1. Default value when this parameter is omitted:

All the lower 12 digits of additional information are monitored.

2. Range of values:

Specify a hexadecimal number of 12 digits or less.

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 setting information with this command, at least one of monitoring condition parameters must be specified.

2. Either operation message monitoring or timer monitoring set by the "event timer" command can be set for each applet.

3. If a relevant applet deletes this command while an action set by the "action" command is running, the action will be executed until the end, but actions that have not been executed will not be executed.

4. The output contents of message text in operation messages may change when the software version is changed. When the software version is changed, check whether monitoring conditions need to be changed.

Related commands

event timer

priority

disable

action

event timer

Performs timer monitoring.

Timer monitoring includes the cron timer that monitors a specified date and time, and the interval timer that periodically monitors the passage of a certain amount of time.

Syntax

To set information:

event timer {cron <string> | interval <seconds>}

To delete information:

no event timer

Input mode

`(config-applet)`

Parameters

cron <string>

Specifies monitoring conditions for the cron timer.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify the value in the following format. Specify the value with 511 or fewer characters.
`"<minute> <hour> <day> <month> <week>"`

- <minute>

Specifies the monitoring time (minute) from 0 to 59.

- <hour>

Specifies the monitoring time (hour) from 0 to 23.

- <day>

Specifies the monitoring time (day) from 1 to 31.

- <month>

Specifies the monitoring time (month) from 1 to 12.

- <week>

Specifies the monitoring time (day of the week) from 0 to 7. The days of the week indicated by each value are as follows.

0=Sunday, 1=Monday, 2=Tuesday, 3=Wednesday

4=Thursday, 5=Friday, 6=Saturday, 7=Sunday

In addition, the following symbols can be specified for each item.

- Wildcard (*)

All the values that can be specified for each item are specified.

- Comma (,)

Multiple numbers can be specified by separating each with a comma.

- Slash (/)

   Monitors are performed at intervals of the number specified on the right of a slash.

- Hyphen (-)

   The range of values can be specified by inserting a hyphen between numbers.

The following table shows examples of specifying <string>.

Table 14-1: Examples of specifying <string>

Specified value	Monitoring condition
"* * * * *"	Runs every minute.
"43 23 * * *"	Runs every day at 23:43.
"0 17 * * 1"	Runs every Monday at 17:00.
"0,10 17 * * 0,2,3"	Runs every Sunday, Tuesday, and Wednesday at 17:00 and 17:10.
"0-10 17 1 * *"	Runs every minute from 17:00 to 17:10 on the 1st day of every month.
"0 0 1,15 * 1"	Runs at 0:00 on the 1st and 15th days of every month and on Mondays.
"42 4 1 * *"	Runs at 4:42 on the 1st day of every month.
"0 21 * * 1-6"	Runs every Monday to Saturday at 21:00.
"0,10,20,30,40,50 * * * *"	Runs at 0, 10, 20, 30, 40, and 50 minutes past every hour.
"*/10 * * * *"	Runs every 10 minutes from 0 minute past every hour.
"* 1 * * *"	Runs every minute from 1:00 to 1:59 every day
"0 */1 * * *"	Runs at 0 minute past every hour
"0 * * * *"	Runs at 0 minute past every hour
"2 8-20/3 * * *"	Runs daily at 8:02, 11:02, 14:02, 17:02, and 20:02
"30 5 1,15 * *"	Runs at 5:30 on the 1st and 15th days of every month.

interval <seconds>

Specifies the monitoring time (in seconds) for the interval timer.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 4294967 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 the event management program is restarted, the interval timer will generate events at intervals of the specified time (in seconds) starting from the time of the restart.

2. When the "disable" command or the "no disable" command is executed, or when the "priority" command is executed to set or change the applet execution priority, the interval timer will generate events at intervals of the specified time (in seconds) starting from the time of the command execution.

3. Either timer monitoring or operation message monitoring set by the "event sysmsg" command can be set for each applet.

4. If a relevant applet deletes this command while an action set by the "action" command is running, the action will be executed until the end, but actions that have not been executed will not be executed.

Related commands

event sysmsg

priority

disable

action

priority

Sets the priority of applet execution.

Syntax

To set or change information:

priority {high | normal | low | last}

To delete information:

no priority

Input mode

`(config-applet)`

Parameters

{high | normal | low | last}

Specifies the priority of applet execution.

high

Sets the priority of applet execution to high (The level of the priority is 6).

normal

Sets the priority of applet execution to medium (The level of the priority is 3).

low

Sets the priority of applet execution to low (The level of the priority is 1).

last

Sets the priority of applet execution to last. This priority notification is sent when there are no longer other priority notifications.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The priority of applet execution is set to medium.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of 1024 events for each execution priority are queued as waiting for action execution. Therefore, if events occur frequently, events may be discarded, and actions may not be executed.

2. If you change the setting of this command for a relevant applet while an action set by the "action" command is running, the action will be executed until the end, but actions that have not been executed will not be executed.

Related commands

event timer

event sysmsg

disable

action

resident-script

Specifies startup information for a resident script.

Syntax

To set information:

resident-script <script id> python <file name> [<args>...]

To delete information:

no resident-script <script id>

Input mode

`(config)`

Parameters

<script id>

Specifies a script ID that identifies a resident script.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 4

python <file name>

Specifies a Python script to be started.

<file name>

Specifies the file name of the Python script.

The file installed by the "install script" operation command is started.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify a string of no more than 99 characters including the extension (either ".py", ".pyc", or ".pyo").

Characters that can be used are alphanumeric characters, dots (.), hyphens (-), underscores (_), tildes (~), and hats (^).

<args>...

Specifies command line arguments to be given at the Python script startup.

1. Default value when this parameter is omitted:

None

2. Range of values:

An <args> can be specified with a maximum of 63 characters. Up to 32 <args> can be registered.

Specifiable characters are alphanumeric characters and special characters. If you specify multiple <args>, specify them separating each with a space. If you use special characters such as a space in an <args>, enclose the string of the <args> in double quotation marks ("). For details, see "■Arbitrary 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

None

15 **Ethernet**

bandwidth

Assigns the bandwidth of a line. This setting is used for calculating the line usage rate on a network monitoring device.

Syntax

To set or change information:

> bandwidth <kbit/s>

To delete information:

> no bandwidth

Input mode

`(config-if)`

> Ethernet interface

Parameters

<kbit/s>

> Assigns the line bandwidth in kbit/s.
>
> This setting is used for the ifSpeed/ifHighSpeed/axsIfStatsHighSpeed (SNMP MIB) value of the applicable port, and has no impact on communication.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 100000000
>
>   Do not specify a value that exceeds the line speed of the applicable port.

Default behavior

The line speed of the applicable port becomes the bandwidth.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

description

Sets supplementary information. This command can be used as a comment about the port. Note that when this command is set, information can be checked by using the "show interfaces" operation command or if-Descr (SNMP MIB).

Syntax

To set or change information:

description <string>

To delete information:

no description

Input mode

`(config-if)`

Ethernet interface

Parameters

<string>

Sets supplementary information for an Ethernet interface.

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 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 "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

null 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

None

duplex

Sets the duplex mode for the following Ethernet interfaces:

- 10BASE-T/100BASE-TX/1000BASE-T
- 100BASE-TX/1000BASE-T/10GBASE-T
- SFP ports used for 10BASE-T/100BASE-TX/ 1000BASE-T or 1000BASE-X
- SFP+/SFP shared ports used for 10BASE-T/100BASE-TX/ 1000BASE-T or 1000BASE-X

Syntax

To set or change information:

duplex { auto | full }

To delete information:

no duplex

Input mode

(config-if)

Ethernet interface

Parameters

{ auto | full }

Sets the connection mode of a port to full duplex (fixed) or auto-negotiation.

auto

Determines the duplex mode by auto-negotiation.

full

Sets the port to full duplex (fixed) mode.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

auto is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied when the command is set.

Notes

1. When 10GBASE-R is used, the duplex and speed settings become disabled.

2. For 1000BASE-X, if auto-negotiation is not used, you must set speed to 1000 and duplex to full. If the auto or auto 1000 parameter is specified in the "speed" command, full is set for duplex as a result of the auto-negotiation.

3. For 1000BASE-T and 10GBASE-T, the setting of duplex changes to auto, and full duplex is supported as a result of auto-negotiation.

4. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.

Related commands

speed

flowcontrol

Sets flow control.

Syntax

To set or change information:

flowcontrol send {desired | on | off} [loose]

flowcontrol receive {desired | on | off}

To delete information:

no flowcontrol send

no flowcontrol receive

Input mode

`(config-if)`

Ethernet interface

Parameters

send {desired | on | off}

Specifies the behavior for sending flow-control pause packets. Specify the same settings as those for the behavior for receiving flow-control pause packets at the destination.

desired

If fixed mode is specified, pause packets are sent. If the auto-negotiation function is specified, whether pause packets are sent is determined through communication with the connected device.

on

Pause packets are sent.

off

Pause packets are not sent.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

loose

Loose flow control mode is set.

In loose mode, the pause-packet sending interval is longer than the transmission suppression time.

1. Default value when this parameter is omitted:

Loose mode is not set.

2. Range of values:

None

receive {desired | on | off}

Sets the behavior for receiving flow-control pause packets. Specify the same settings as those for the behavior for sending flow-control pause packets at the destination.

desired

If fixed mode is set, pause packets are received. If the auto-negotiation function is specified, whether pause packets are received is determined through communication with the connected device.

on

Pause packets are received.

off

Pause packets are not received.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

Behavior varies depending on the line type.

- For 10BASE-T, 100BASE-TX, or 1000BASE-T:

  The receive behavior is off but the send behavior is desired.

- For 100BASE-TX, 1000BASE-T, or 10GBASE-T:

  The receive behavior is off but the send behavior is desired.

- For 1000BASE-X:

  The receive behavior is off but the send behavior is desired.

- For 10GBASE-R:

  The receive behavior is on but the send behavior is off.

- For 40GBASE-R:

  The receive behavior is on but the send behavior is off.

- For 100GBASE-R:

  The receive behavior is on but the send behavior is off.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

frame-error-notice

Sets the condition for sending a notification when a frame reception error or a frame sending error occurs. A frame reception error or a frame sending error indicates that a frame is discarded due to a failure in receiving or sending a frame, which is caused by a minor error. The cause of the failure is collected as statistics. If the number of error occurrences or the error occurrence rate over 30 seconds exceeds the value set by using this command, the error occurrences are reported. The settings of this command are applied to all ports of the Switch, and the sending side and the receiving side have the same settings.

If this configuration is not set, the error occurrences are reported when 15 or more errors occur in a 30-second interval.

The following table shows the list of error items that correspond to frame reception and frame sending errors.

Table 15-1: List of error items

No.	Error items	
	Receiving	**Sending**
1	• CRC errors • Alignment • Fragments • Jabber • Symbol errors • Short frames • Long frames	• Late collision • Excessive collisions • Excessive deferral

If an error occurrence is reported, a log entry is displayed and a private SNMP notification is sent. For details about logs, see the "Message Log Reference".

Syntax

To set or change information:

frame-error-notice [error-frames <frames>] [error-rate <rate>] [{ one-time-display | everytime-display | off }]

Note: At least one parameter must be specified.

To delete information:

no frame-error-notice

Input mode

(config)

Parameters

error-frames <frames>

Sets, as the error notification condition, the threshold for the number of error occurrences (number of error frames).

1. Default value when this parameter is omitted:

15

2. Range of values:

1 to 446400000

error-rate \<rate\>

Specifies, as the error notification condition, the threshold for the error occurrence rate as a percentage (%). The error occurrence rate is calculated as the rate of the number of error frames against the total number of frames. The fractional portion of the rate is truncated, and then it is compared with the set value. Note that if this parameter is omitted, the error occurrence rate is not regarded as a notification condition.

1. Default value when this parameter is omitted:

   The error occurrence rate is not regarded as a notification condition.

2. Range of values:

   1 to 100

The notification condition varies depending on whether the error-frames parameter and/or the error-rate parameter are set. The following table shows the error notification conditions depending on whether each parameter is set.

Table 15-2: List of error notification conditions

No.	Parameter		Receiving/send-ing	Error notification condition
	error-frames	error-rate		
1	Omitted	Omitted	Receiving	The number of reception error frames is 15 or more.
2			Sending	The number of sending error frames is 15 or more.
3		Set	Receiving	The rate of reception error frames against the total number of reception frames is equal to or greater than the value set for \<rate\>. This setting does not regard the number of error occurrences as a notification condition.
4			Sending	The rate of sending error frames against the total number of sending frames is equal to or greater than the value set for \<rate\>. This setting does not regard the number of error occurrences as a notification condition.
5	Set	Omitted	Receiving	The number of reception error frames is equal to or greater than the value set for \<frames\>. This setting does not regard the error occurrence rate as a notification condition.
6			Sending	The number of sending error frames is equal to or greater than the value set for \<frames\>. This setting does not regard the error occurrence rate as a notification condition.
7		Set	Receiving	The number of reception error frames is equal to or greater than the value set for \<frames\>, and the rate of reception error frames against the total number of reception frames is equal to or greater than the value set for \<rate\>.
8			Sending	The number of sending error frames is equal to or greater than the value set for \<frames\>, and the rate of sending error frames against the total number of sending frames is equal to or greater than the value set for \<rate\>.

{ everytime-display | one-time-display | off }

Specifies whether to display a log entry when an error occurrence is reported. If a large number of errors occur continuously, this setting can prevent the log file from being filled with this log entry. Note that this parameter has no impact on private SNMP notifications. Use the "snmp-server host" command to specify whether to send a private SNMP notification. For details, see "snmp-server host" command.

everytime-display

Displays a log entry every time an error occurrence is reported.

one-time-display

Displays a log entry only when an error occurrence is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error occurrence after the restart is reported.

off

No log entries are displayed.

1. Default value when this parameter is omitted:

one-time-display

2. Range of values:

None

Default behavior

When 15 or more errors occur in a 30-second time interval, the error occurrences are reported. Displays a log entry only when an error occurrence is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error occurrence after the restart is reported.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you use this command to set the configuration, you must specify at least one parameter.

2. Entering this command disables the settings specified until then. If you want to inherit the old settings, use this command to specify the applicable parameter again.

Related commands

snmp-server host

interface fortygigabitethernet

Entering this command switches to config-if mode, in which information about 40 Gbit/s Ethernet interfaces, which can be used only as stack ports, can be set. Note that this command is set only when the stack function is enabled on the model with stack-dedicated ports.

Syntax

To set information:

interface fortygigabitethernet <switch no.>/<nif no.>/<port no.>

Input mode

(config)

Parameters

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and the port number.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

None

Related commands

stack enable

interface gigabitethernet

Sets the items related to an Ethernet interface that has a maximum line speed of 1000 Mbit/s. Entering this command switches to config-if mode, in which information about the relevant port can be set.

Specifying a subinterface with this command switches to config-subif mode, in which various information about Ethernet subinterfaces can be set. Subinterface settings is enabled for the VXLAN function. [SL-L3A]

Syntax

To set information:

interface gigabitethernet <switch no.>/<nif no.>/<port no.>

interface gigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>

To delete information:

no interface gigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>

Input mode

`(config)`

Parameters

<switch no.>/<nif no.>/<port no.>

Specifies the switch number, NIF number, and the port number.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

<switch no.>/<nif no.>/<port no.>.<subinterface index> [SL-L3A]

Specifies the switch number, NIF number, port number, and subinterface index.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. When setting a subinterface, first set the "no switchport" command on an appropriate interface.
   [SL-L3A]

Related commands

switchport [SL-L3A]

interface hundredgigabitethernet

Sets items related to an Ethernet interface that has a maximum line speed of 100 Gbit/s. Entering this command switches to config-if mode, in which information about the relevant port can be set.

Specifying a subinterface with this command switches to config-subif mode, in which various information about Ethernet subinterfaces can be set. Subinterface settings is enabled for the VXLAN function. [SL-L3A]

Syntax

To set information:

> interface hundredgigabitethernet <switch no.>/<nif no.>/<port no.>

> interface hundredgigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>

To delete information:

> no interface hundredgigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>

Input mode

`(config)`

Parameters

<switch no.>/<nif no.>/<port no.>

> Specifies the switch number, NIF number, and the port number.

>> 1. Default value when this parameter is omitted:

>> This parameter cannot be omitted.

>> 2. Range of values:

>> See "Specifiable values for parameters".

<switch no.>/<nif no.>/<port no.>.<subinterface index> [SL-L3A]

> Specifies the switch number, NIF number, port number, and subinterface index.

>> 1. Default value when this parameter is omitted:

>> This parameter cannot be omitted.

>> 2. Range of values:

>> See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. When setting a subinterface, first set the "no switchport" command on an appropriate interface.
   [SL-L3A]

Related commands

switchport [SL-L3A]

interface tengigabitethernet

Sets items related to an Ethernet interface that has a maximum line speed of 10 Gbit/s. Entering this command switches to config-if mode, in which information about the relevant port can be set.

Specifying a subinterface with this command switches to config-subif mode, in which various information about Ethernet subinterfaces can be set. Subinterface settings is enabled for the VXLAN function. [SL-L3A]

Syntax

To set information:

> interface tengigabitethernet <switch no.>/<nif no.>/<port no.>

> interface tengigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>

To delete information:

> no interface tengigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>

Input mode

`(config)`

Parameters

<switch no.>/<nif no.>/<port no.>

> Specifies the switch number, NIF number, and the port number.

>> 1. Default value when this parameter is omitted:

>> This parameter cannot be omitted.

>> 2. Range of values:

>> See "Specifiable values for parameters".

<switch no.>/<nif no.>/<port no.>.<subinterface index> [SL-L3A]

> Specifies the switch number, NIF number, port number, and subinterface index.

>> 1. Default value when this parameter is omitted:

>> This parameter cannot be omitted.

>> 2. Range of values:

>> See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. For the AX3660S-24T4XW and AX3660S-48T4XW models, 10GBASE-R can be used only when the software license or optional license supports 10G uplink.

2. When setting a subinterface, first set the "no switchport" command on an appropriate interface. [SL-L3A]

Related commands

switchport [SL-L3A]

link debounce

Sets the link-down detection time after a link failure is detected until the actual link-down occurs. When a large value is set, temporary link-downs will not be detected, thereby preventing instability of the link.

Syntax

To set or change information:

link debounce [time <milli seconds>]

To delete information:

no link debounce

Input mode

`(config-if)`

Ethernet interface

Parameters

time <milli seconds>

Sets the debounce timer value in milliseconds.

1. Default value when this parameter is omitted:

3000 milliseconds

2. Range of values:

Multiples of 100 from 0 to 10000

Default behavior

The value is set to 2000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the link is stable even when a link-down detection timer is not set, you do not need to set one.

2. If a value smaller than the default value (2000 milliseconds) is set for 10BASE-T/100BASE-TX/ 1000BASE-T/10GBASE-T/10GBASE-CU/40GBASE-CR4/100GBASE-CR4, the link might become unstable.

Related commands

None

link up-debounce

Sets the link-up detection time after a link failure is detected until the actual link-up occurs. When a large value is set, a temporary link-up will not be detected, thereby preventing instability of the network status.

Syntax

To set or change information:

> link up-debounce time <milli seconds>

To delete information:

> no link up-debounce

Input mode

`(config-if)`

> Ethernet interface

Parameters

time <milli seconds>

> Sets the debounce timer value when a link-up state occurs, in milliseconds.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   Multiples of 100 from 0 to 10000

Default behavior

When the line speed is fixed, the value is set to 1000 milliseconds. When the line speed is set to auto-negotiation, the value is set to 0 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The larger the value you set for the link-up detection timer, the more time it takes until communication is restored after a link failure has been corrected. If you want this time to be short, do not set a link-up detection timer.

2. If you set a value smaller than the default value, the link might become unstable.

Related commands

link debounce

speed

duplex

mdix auto

Sets the AUTO-MDI/MDI-X function of the port to be used. When no mdix auto is specified, the AUTO-MDI/MDI-X function is disabled and the port is fixed to MDI-X.

Syntax

To set information:

> no mdix auto

To delete information:

> mdix auto

Input mode

`(config-if)`

> Ethernet interface

Parameters

None

Default behavior

During auto-negotiation, MDI and MDI-X are switched automatically.

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 during auto-negotiation.
2. For 1000BASE-X, this command is disabled.
3. For 10GBASE-R, this command is disabled.
4. For 40GBASE-R, this command cannot be specified.
5. For 100GBASE-R, this command cannot be specified.

Related commands

speed

mtu

Sets the MTU for ports. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

 mtu <length>

To delete information:

 no mtu

Input mode

`(config-if)`

 Ethernet interface

Parameters

 Sets the MTU of ports in octets. The MTU is the maximum length of the data section[#] for frames in Ethernet V2 format.

 #: For details on the frame format, see "Configuration Guide Vol.1, 20.2.2 Frame format".

 1. Default value when this parameter is omitted:

  This parameter cannot be omitted.

 2. Range of values:

  1500 to 9216

Default behavior

The following initial values are set.

Table 15-3: Initial MTU values for ports

Presence of the system mtu command	Initial value
Set	Setting value for system mtu
Not set	1500

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the MTU of the applicable port and the length of frames that can be sent or received (the maximum length of frames in Ethernet V2 format[#], excluding the FCS).

   #: For details on the frame format, see "Configuration Guide Vol.1, 20.2.2 Frame format".

   Table 15-4: MTU and the length of frames that can be sent or received

Line type	mtu setting	system mtu Method	Length of frames that can be sent or received (octets)	Port MTU (octets)
10BASE-T	Not related	Not related	Tagged 1518 Untagged 1518	1500
Other	Set	Not related	Tagged $M1^{\#1}+18$ Untagged $M1^{\#1}+18$	$M1^{\#1}$
	Not set	Set	Tagged $M2^{\#2}+18$ Untagged $M2^{\#2}+18$	$M2^{\#2}$
		Not set	Tagged 1518 Untagged 1518	1500

   #1: The value set by using the "mtu" command of interface

   #2: The value set by using the "system mtu" command

2. Use the same MTU value for the ports belonging to the VLAN. If the MTU is different, frame forwarding is performed as follows:

   - For L2 forwarding, if the MTU of the sending port is smaller than the MTU of the receiving port, the length of a frame to be forwarded is up to 4 octets longer than the length of a frame that can be sent or received on the sending port.

   - For L3 forwarding, the MTU for a VLAN interface varies depending on the port MTU and the IP MTU setting.

   Table 15-5: MTU for a VLAN interface

MTU setting	IP MTU setting	MTU of a VLAN interface (in octets)
Omitted	Omitted	1500
	Set	$\min(1500, L2^{\#1})$
Set	Omitted	$L1^{\#2}$
	Set	$\min(L1^{\#2}, L2^{\#1})$

   #1: IP MTU value

   #2: Port MTU value (if values differ among ports, the minimum value is used.)

3. For two row VLAN tags in VLAN tunneling, the frame length will be "IP packet length + 22 octets". If an IP packet of 1500 octets is sent from a port with two-row VLAN tags, set a value equal to or larger than 1504 for mtu.

Related commands

None

network-clock input-source

Enable Sync-E and set a receiving port number for an external clock.

Syntax

To set information:

> network-clock input-source \<priority\> interface tengigabitethernet \<switch no.\>/\<nif no.\>/\<port no.\>

To delete information:

> no network-clock input-source \<priority\> interface tengigabitethernet \<switch no.\>/\<nif no.\>/\<port no.\>

Input mode

`(config)`

Parameters

\<priority\>

> Sets the priority of the specified interface. The lower the value, the higher the priority.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 or 2

interface tengigabitethernet \<switch no.\>/\<nif no.\>/\<port no.\>

> Specifies the receiving port number for an external clock.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".

Default behavior

Sync-E is disabled. The internal clock is enabled for all ports.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the receiving port for the external clock, an SFP+/SFP shared port can only be specified.

2. For a port that has already been specified as a receiving port for the external clock, the priority cannot be changed.

Related commands

None

network-clock preempt-delay

Sets the automatic switchback suppression time for receiving ports with Sync-E. This setting is applied when the synchronization destination of the clock frequency to be used is changed as follows.

- Changed from a low-priority port to high-priority port
- Changed from the internal clock to the external clock

Syntax

To set or change information:

> network-clock preempt-delay <seconds>

To delete information:

> no network-clock preempt-delay

Input mode

`(config)`

Parameters

<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 automatic switchback suppression time is 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The time set by this command is applied to both high-priority and low-priority ports.

2. If this command is set or changed during automatic switchback suppression, the suppression time will be cleared and suppression will start again from the time when the command is set.

3. When the "network-clock input-source" command is set, the use of the external clock starts after the time set by this command has passed.

4. If a high-priority port is in automatic switchback suppression and a low-priority port is in one of the following states, the high-priority port ends switchback suppression and synchronizes with the external clock.

- The automatic switchback suppression time has expired.
- The reception status of the external clock changed from Lock to Unlock during synchronization with the external clock.

5. The automatic switchback suppression time may deviate from the set time if the CPU load is high. The delay should be less than one minute.

Related commands

None

shutdown

Places the port in the shutdown state.

Syntax

To set information:

shutdown

To delete information:

no shutdown

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

Communication using the relevant port becomes unavailable.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

2. When the scheduled power saving function is in use, the device works according to the configuration of the "schedule-power-control shutdown" command.

Related commands

None

speed (gigabitethernet)

Sets the speed of a port for the following Ethernet interfaces:

- 10BASE-T/100BASE-TX/1000BASE-T
- SFP ports used for 10BASE-T/100BASE-TX/ 1000BASE-T or 1000BASE-X

Syntax

To set or change information:

> speed { 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

To delete information:

> no speed

Input mode

`(config-if)`

> Ethernet interface

Parameters

{ 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

> Sets the line speed.
>
> The table below shows the combinations of line types and specifiable parameters.
>
> auto is set if a non-specifiable parameter for 10BASE-T, 100BASE-TX, 1000BASE-T, or 1000BASE-X is specified.

Table 15-6: Specifiable parameters

Line type	Specifiable parameters
10BASE-T/ 100BASE-TX/ 1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
1000BASE-X	1000 auto auto 1000

> 10
>
> > Sets the line speed to 10 Mbit/s.
>
> 100
>
> > Sets the line speed to 100 Mbit/s.
>
> 1000
>
> > Sets the line speed to 1000 Mbit/s.

Sets the line speed to auto-negotiation.

auto {10 | 100 | 1000 | 10 100 | 10 100 1000}

Auto-negotiation is performed at the specified line speed. This setting prevents the line speed from operating at an unexpected speed, so the line usage rate is prevented from increasing. If negotiation at the specified line speed does not succeed, the link status does not transition to link-up status.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

auto is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.

2. If auto-negotiation is not used for 10BASE-T, 100BASE-TX, or 1000BASE-T, you must set speed to 10 or 100, and set duplex to full.

3. For 1000BASE-X, if auto-negotiation is not used, you must set speed to 1000 and duplex to full.

Related commands

duplex

speed (tengigabitethernet)

Sets the speed of a port for the following Ethernet interfaces:

- 100BASE-TX/1000BASE-T/10GBASE-T

- SFP+/SFP shared ports used for 10BASE-T/100BASE-TX/ 1000BASE-T or 1000BASE-X

Syntax

To set or change information:

speed {10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10000 | 10 100 | 10 100 1000 | 100 1000 | 100 1000 10000}}

To delete information:

no speed

Input mode

`(config-if)`

Ethernet interface

Parameters

{10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10000 | 10 100 | 10 100 1000 | 100 1000 | 100 1000 10000}}

Sets the line speed.

The table below shows the combinations of line types and specifiable parameters.

auto is set if a non-specifiable parameter for any line speed.

Table 15-7: Specifiable parameters

Line type	Specifiable parameters
10BASE-T/100BASE-TX/1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
100BASE-TX/1000BASE-T/10GBASE-T	100 auto auto 100 auto 1000 auto 10000 auto 100 1000 auto 100 1000 10000
1000BASE-X	1000 auto

Line type	Specifiable parameters
	auto 1000

10

Sets the line speed to 10 Mbit/s.

100

Sets the line speed to 100 Mbit/s.

1000

Sets the line speed to 1000 Mbit/s.

auto

Sets the line speed to auto-negotiation.

auto {10 | 100 | 1000 | 10000 | 10 100 | 10 100 1000 | 100 1000 | 100 1000 10000}

Auto-negotiation is performed at the specified line speed. This setting prevents the line speed from operating at an unexpected speed, so the line usage rate is prevented from increasing. If negotiation at the specified line speed does not succeed, the link status does not transition to link-up status.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

auto is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied when the command is set.

Notes

1. When 10GBASE-R is used, the duplex and speed settings become disabled.

2. For 1000BASE-X, if auto-negotiation is not used, you must set speed to 1000 and duplex to full.

3. If auto-negotiation is not used for 10BASE-T, 100BASE-TX, or 1000BASE-T, you must set speed to 10 or 100, and set duplex to full.

4. If auto-negotiation is not used for 100BASE-TX, 1000BASE-T, or 10GBASE-T, you must set speed to 100, and set duplex to full.

5. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.

Related commands

duplex

system flowcontrol off

Disables flow control for all ports on the device. This setting has priority over flow control settings for specific ports.

Syntax

To set information:

 system flowcontrol off

To delete information:

 no system flowcontrol off

Input mode

`(config)`

Parameters

None

Default behavior

The flow control setting specified for each port is used.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

Restarting the VLAN program re-initializes all ports, and the ports that make up the VLAN temporarily become unable to send or receive data.

When the change is applied

If you have changed any values, save the configuration and restart the Switch or VLAN program. The new setting values take effect when the Switch is restarted.

Notes

None

Related commands

flowcontrol

system minimum-tagged-frame-length-68

Sets the minimum frame length of tagged frames spontaneously sent by the switch and relayed by software to 68 octets. Even if this configuration is set, tagged 64-octet frames are not discarded.

Syntax

To set information:

system minimum-tagged-frame-length-68

To delete information:

no system minimum-tagged-frame-length-68

Input mode

`(config)`

Parameters

None

Default behavior

If this command is not specified, the minimum frame length of tagged frames spontaneously sent by the switch and relayed by software is set to 64 octets.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

system mtu

Sets the MTU of all ports. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

> system mtu <length>

To delete information:

> no system mtu

Input mode

`(config)`

Parameters

> Sets the MTU of all ports in octets. The MTU is the maximum length of the data section[#] for frames in Ethernet V2 format.
>
> #: For details on the frame format, see "Configuration Guide Vol.1, 20.2.2 Frame format".
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
> 2. Range of values:
>
>   1500 to 9216 (octets)

Default behavior

The MTU of all ports is set to 1500.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the port MTU and the length of a frame that can be sent or received (the maximum length of a frame in Ethernet V2 format[#], excluding the FCS).

   #: For details on the frame format, see "Configuration Guide Vol.1, 20.2.2 Frame format".

Table 15-8: MTU and the length of frames that can be sent or received

Line type	mtu setting	system mtu setting	Length of a frame that can be sent or received (in octets)	Port MTU (in octets)
10BASE-T	Not related	Not related	Tagged 1518 Untagged 1518	1500
Other	Set	Not related	Tagged $M1^{\#1}+18$ Untagged $M1^{\#1}+18$	$M1^{\#1}$
	Not set	Set	Tagged $M2^{\#2}+18$ Untagged $M2^{\#2}+18$	$M2^{\#2}$
		Not set	Tagged 1518 Untagged 1518	1500

#1: The value set by using the "mtu" command of interface

#2: The value set by using the "system mtu" command

2. For two row VLAN tags in VLAN tunneling, the frame length will be "IP packet length + 22 octets". If an IP packet of 1500 octets is sent from a port with two-row VLAN tags, set system mtu so that the port mtu value is set to a value larger than 1504 or set mtu on the port.

Related commands

None

16 Link Aggregation

channel-group lacp system-priority

Sets the LACP system priority of the applicable channel group for link aggregation.

Syntax

To set or change information:

channel-group lacp system-priority <priority>

To delete information:

no channel-group lacp system-priority

Input mode

`(config-if)`

Port channel interface

Parameters

<priority>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 65535

Default behavior

The setting of the "lacp system-priority" command is used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down, and then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.

2. If you set a function to restrict the number of detached ports (max-detach-port) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.

3. If the LACP system priority is changed, the status of all ports registered for the channel group changes to Blocking (communication interrupted).

Related commands

channel-group max-detach-port

channel-group max-active-port

Sets the maximum number of active ports that will be used for link aggregation in the applicable channel group.

Syntax

To set information:

channel-group max-active-port <number> [no-link-down]

To change information:

channel-group max-active-port <number>

channel-group max-active-port <number> no-link-down

To delete information:

no channel-group max-active-port

Input mode

`(config-if)`

Port channel interface

Parameters

<number>

Specifies the maximum number of ports that will be used for link aggregation in a channel group. If the number of ports that are actually used in a channel group exceeds the value specified by this command, only the specified maximum number of ports are used, and the standby link function is applied to the rest of the ports.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 8

no-link-down

To use the standby link function in a link-not-down mode, specify this parameter. Otherwise, standby links switch to the link-down status. The criteria for selecting which links are standby links are as follows:

- Select ports that have been assigned lower priority by using the "lacp port-priority" command.
- If the priority is the same, select the port with the larger switch number, larger NIF number, and larger port number.

1. Default value when this parameter is omitted:

Standby links switch to link-down status.

2. Range of values:

None

Default behavior

The maximum number is 8.

Impact on communication

The ports that are in use might be changed by the standby link function, and communication might stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when static link aggregation is used.

2. If you specify the "max-active-port" command, match its settings to the settings of the "max-active-port" and "lacp port-priority" commands on the destination device.

3. Ports in standby link mode cannot be changed directly between the link-down and no-link-down statuses. To change the status, delete this parameter, and then set this parameter again. To change the number of ports in a link-not-down mode, you must specify the no-link-down parameter.

4. If this command is set and a port in link-down status is selected as a standby link, only the log entries that indicate detachment are displayed. Log entries indicating aggregation for the ports are not displayed.

Related commands

channel-group lacp system-priority

lacp system-priority

lacp port-priority

channel-group max-detach-port

Limits the maximum number of detached ports in the applicable link aggregation channel group.

Syntax

To set or change information:

channel-group max-detach-port <number>

To delete information:

no channel-group max-detach-port

Input mode

`(config-if)`

Port channel interface

Parameters

<number>

Specifies the maximum number of ports that can be detached from a channel group used for link aggregation for reasons such as a link down. When 0 is specified, no ports can be detached. Therefore, if a link goes down, the whole channel group goes down.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 or 7

Default behavior

7 is set as the limit on the maximum number of detached ports.

Impact on communication

Channel groups might go down due to a function to restrict the number of detached ports.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.

2. If you specify the "max-detach-port" command, match its settings to the settings of the destination device.

3. If 0 is entered for the "max-detach-port" command, the effect is the same as when 7 is entered for the "max-detach-port" command in on mode (this is the default when nothing is entered for max-detach-port).

4. If you set a function to restrict the number of detached ports (max-detach-port) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.

5. If you change the value for <number> to 0, all ports registered for the channel group change to Blocking (communication interrupted) while some ports registered in the channel group for the applicable link aggregation are degraded.

Related commands

channel-group mode

channel-group lacp system-priority

lacp system-priority

channel-group mode

Creates a channel group for link aggregation.

Syntax

To set information:

channel-group <channel group number> mode { on | { active | passive } }

To change information:

channel-group <channel group number> mode { active | passive }

To delete information:

no channel-group

Input mode

`(config-if)`

Ethernet interface

Parameters

<channel group number>

Specifies the channel group number for link aggregation.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

mode { on | { active | passive } }

Specifies the mode for link aggregation.

on

Static link aggregation is performed.

active

LACP-based link aggregation is performed, and LACPDUs are always sent irrespective of the remote device.

passive

LACP-based link aggregation is performed, but LACPDUs are sent only when an LACPDU from the remote device is received.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

None

Impact on communication

If this setting is specified for an active port, communication temporarily stops.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To change static link aggregation to LACP-based link aggregation, or vice versa, delete this command, change the mode, and then set the command again.

2. When channel-group mode is set, the port-channel setting of the specified channel group is automatically generated. If port-channel has already been set, no specific operation is required.

3. If the port-channel setting of the specified channel group number already exists when you set this command, you must either specify the same setting for the applicable interface and the port channel interface with the specified channel group number or else not set a common configuration command for the applicable interface. For details, see "Configuration Guide Vol. 1, 21.2.4 Configuring a port channel interface".

4. If you want to delete this command, do so after executing the "shutdown" command for the applicable interface.

5. Deleting this command does not delete the port-channel configuration (deleting all ports in a channel group does not delete the port-channel configuration). When deleting a channel group, you must delete the port-channel configuration manually.

Related commands

None

channel-group multi-speed

Sets mixed-speed mode. If this command is set, ports with different transmission speeds can be used simultaneously in a channel group for link aggregation.

Syntax

To set information:

channel-group multi-speed

To delete information:

no channel-group multi-speed

Input mode

`(config-if)`

Port channel interface

Parameters

None

Default behavior

None

Impact on communication

The ports that are in use might be changed by the standby link function, and communication might stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When frames are sent, ports are allocated irrespective of the port transmission speed.

Related commands

None

channel-group periodic-timer

Specifies the interval for sending LACPDUs.

Syntax

To set or change information:

> channel-group periodic-timer { long | short }

To delete information:

> no channel-group periodic-timer

Input mode

`(config-if)`

> Port channel interface

Parameters

{ long | short }

> Specifies the sending interval at which the partner device sends LACPDUs to a Switch.
>
> long: 30 seconds
>
> short: one second
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
> 2. Range of values:
>
>   None

Default behavior

long (30 seconds) is set as the sending interval.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.

Related commands

channel-group mode

description

Sets supplementary information.

Syntax

To set or change information:

description <string>

To delete information:

no description

Input mode

`(config-if)`

Port channel interface

Parameters

<string>

Sets supplementary information for the applicable channel group used for link aggregation. Use this command to create and attach a note to the interface.

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 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 "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

NULL 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

None

interface port-channel

Sets an item related to a port channel interface. Entering this command switches to config-if mode, in which configuration commands can be set to specify the channel group number. A port channel interface is automatically generated when the "channel-group mode" command is set.

Specifying a subinterface with this command switches to config-subif mode, in which various information about port channel subinterfaces can be set. Subinterface settings is enabled for the VXLAN function. [SL-L3A]

Syntax

To set information:

interface port-channel <channel group number>

interface port-channel <channel group number>.<subinterface index>

To delete information:

no interface port-channel <channel group number>

no interface port-channel <channel group number>.<subinterface index>

Input mode

`(config)`

Parameters

<channel group number>

Specifies the channel group number.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

<channel group number>.<subinterface index> [SL-L3A]

Specifies the channel group number and subinterface index.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you want to delete this command, do so after executing the "shutdown" command for all ports in the applicable channel group.

2. When setting a subinterface, first set the "no switchport" command on an appropriate interface. [SL-L3A]

Related commands

switchport [SL-L3A]

lacp port-priority

Sets the port priority.

Syntax

To set or change information:

lacp port-priority \<priority>

To delete information:

no lacp port-priority

Input mode

`(config-if)`

Ethernet interface

Parameters

\<priority>

Specifies the port priority. The lower the value, the higher the priority.

When on is specified for the "channel-group mode" command

This parameter is used with the "max-active-port" command to select the standby links.

When active or passive is set for the "channel-group mode" command

This parameter applies to port priority for the LACP protocol.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

0 to 65535

Default behavior

128 is set as the port priority.

Impact on communication

If you specify the port priority for an active port by setting channel-group mode to active or passive, communication is temporarily interrupted. If you specify port priority for active ports by setting channel-group mode to on, ports that are use might be changed by the standby link function, and communication might temporarily stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you specify the "max-active-port" command, match its settings to the settings of max-active-port for the destination device.

2. If you change \<priority>, the status of the applicable port changes to Blocking (communication interrupted).

Related commands

channel-group mode

channel-group max-active-port

lacp system-priority

Sets the effective LACP system priority for a device.

Syntax

To set or change information:

    lacp system-priority <priority>

To delete information:

    no lacp system-priority

Input mode

`(config)`

Parameters

<priority>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

2. Range of values:

    1 to 65535

Default behavior

If the "channel-group lacp system-priority" command has been set, that setting is used. If the "channel-group lacp system-priority" command has not been set, 128 is used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down, and then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.

2. If you set a function to restrict the number of detached ports (max-detach-port) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.

3. If the LACP system priority is changed, the status of all ports registered for the channel group changes to Blocking (communication interrupted).

Related commands

channel-group max-detach-port

port-channel load-balance

For link aggregation, sets the method of allocating frames that are to be sent.

Syntax

To set or change information:

> port-channel load-balance { dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port }

To delete information:

> no port-channel load-balance

Input mode

`(config)`

Parameters

{ dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port }

dst-ip

> Allocates frames according to the destination IP addresses.

dst-mac

> Allocates frames according to the destination MAC addresses. Frames to the same destination address are sent from the same port.

dst-port

> Allocates frames according to the destination port numbers.

src-dst-ip

> Allocates frames according to the source and destination IP addresses.

src-dst-mac

> Allocates frames according to the source and destination MAC addresses.

src-dst-port

> Allocates frames according to the source and destination port numbers.

src-ip

> Allocates frames according to the source IP addresses.

src-mac

> Allocates frames according to the source MAC addresses. Frames from hosts that have the same source MAC address are sent from the same port.

src-port

> Allocates frames according to the source port numbers.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

src-dst-port is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you specify dst-ip, src-dst-ip, or src-ip, TCP/UDP port numbers are not used for allocation in link aggregation, and TCP/IP numbers are not used for path selection in IPv4 multipath routes.

Related commands

None

shutdown

Always disables the applicable channel group for link aggregation, and stops communication.

Syntax

To set information:

shutdown

To delete information:

no shutdown

Input mode

`(config-if)`

Port channel interface

Parameters

None

Default behavior

None

Impact on communication

If a priority is specified for an active channel group, the channel group goes down.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command can be set from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

None

17 **MAC Address Table**

mac-address-move

Sets the move monitoring function for MAC address learning.

Syntax

To set or change information:

mac-address-move detect-count <count> duration <seconds> action {inactivate [auto-recover <seconds>] | log}

To delete information:

no mac-address-move

Input mode

`(config-if)`

Ethernet interface

Parameters

detect-count <count>

Sets the threshold for the number of MAC address learning moves per second for judging whether a loop failure has occurred.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 1000

duration <seconds>

Sets the duration (in seconds) while the number of MAC address learning moves exceeds detect-count for judging whether a loop failure has occurred.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 86400

action {inactivate [auto-recover <seconds>] | log}

Sets an action when the occurrence of a loop failure and recovery from the failure are detected.

inactivate [auto-recover <seconds>]

Deactivates the port when a loop failure is detected. Outputs an operation message when the port status is changed.

auto-recover<seconds> can be used to specify the time (in seconds) before the port is automatically activated since the port is deactivated. If it is omitted, the port will not be automatically activated.

log

Outputs an operation message when the occurrence of a loop failure and recovery from the failure are detected.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

The setting range of <seconds> is 1 to 86400.

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 overwritten and reconfigured, the following parameter settings are used as thresholds to reset the monitoring status and the occurrence status of loop failures.
   - detect-count <count>
   - duration <seconds>
   - auto-recover <seconds>

2. If you not specify auto-recover for action inactivate, use the "activate" operation command to activate the inactive port.

3. If you set an extremely small value for detect-count and duration, MAC address learning moves during normal operation may be misjudged as a loop failure. Adjust the setting values according to your environment.

4. When setting this command for a port belonging to a channel group, make the same setting for all ports belonging to the channel group.

Related commands

None

mac-address-table aging-time

Sets the aging conditions for MAC address table entries.

Syntax

To set or change information:

mac-address-table aging-time <seconds>

To delete information:

no mac-address-table aging-time

Input mode

`(config)`

Parameters

<seconds>

Sets the aging time in seconds. If 0 is specified, aging is not performed.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

0, 10 to 1000000 (seconds)

Default behavior

300 seconds is set as the aging time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A Switch checks for received frames each time the specified aging time elapses. Accordingly, at a maximum, twice the aging time might be required for the learned entries to be deleted.

Related commands

None

mac-address-table learning

The "no mac-address-table learning" command suppresses dynamic MAC address learning for each VLAN or VNI. When MAC address learning is suppressed, frames with non-static entry among frames received in VLANs or VNIs subject to learning suppression are flooded.

Syntax

To set information:

   no mac-address-table learning vlan <vlan id list>

   no mac-address-table learning vni <vni list>

To change information:

   no mac-address-table learning vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

   no mac-address-table learning vni {<vni list> | add <vni list> | remove <vni list>}

To delete information:

   mac-address-table learning vlan

   mac-address-table learning vni

Input mode

`(config)`

Parameters

vlan <vlan id list>

   Specifies the list of VLANs for which MAC address learning is to be suppressed.

   1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

   2. Range of values:

   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

   Modifies the specified VLAN list. add specifies VLANs to be added to the specified VLAN list, and remove specifies VLANs to be removed 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

vni <vni list> [SL-L3A]

   Specifies the list of VNIs for which MAC address learning is to be suppressed.

   1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

   2. Range of values:

For details about how to specify <vni list> and the specifiable range of values, see "Specifiable values for parameters".

vni {<vni list> | add <vni list> | remove <vni list>} [SL-L3A]

Modifies the specified VNI list. add specifies VNIs to be added to the specified VNI list, and remove specifies VNIs to be removed from the specified VNI list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to specify <vni list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

MAC address learning is not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If MAC address learning is suppressed, the MAC address table learned for target VLANs or VNIs is deleted.

2. If MAC address learning suppression is set for a VLAN, the VLAN cannot be used as a Layer 3 interface.

3. If the VXLAN function is disabled, MAC address learning is not suppressed for target VNIs.

Related commands

vlan

vxlan enable [SL-L3A]

member vni [SL-L3A]

mac-address-table static

Sets static MAC address table information.

Syntax

To set or change information:

mac-address-table static <mac> vlan <vlan id> {interface <interface type> <interface number> | drop}

To delete information:

no mac-address-table static <mac> vlan <vlan id>

Input mode

`(config)`

Parameters

<mac>

Specifies a MAC address to be registered as a static entry.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

0000.0000.0000 to feff.ffff.ffff

Note, however, that a multicast MAC address (address whose first-byte lowest bit is set to 1) cannot be set.

vlan <vlan id>

Specifies the VLAN ID of the VLAN for static entries.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

{interface <interface type> <interface number> | drop}

Specifies whether to forward or discard the frames that match the static entry.

interface <interface type> <interface number>

Specifies the output destination interface for static entries.

drop

Specifies that frames are discarded based on the static entry.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

- Ethernet interface

- Port channel interface

Default behavior

No static entries are set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you set a static entry for the default VLAN (VLAN ID = 1), explicitly set "vlan 1" for the output destination interface.

2. If interface has been specified, a frame is output to the interface specified for frames matching the destination MAC address. In addition, if a frame is received from an interface other than the one specified for frames as matching the source MAC address, it is discarded.

3. If drop is specified, the frames matching the destination MAC address or source MAC address are discarded.

4. If a physical port in the channel group is specified as an output destination interface, communication might not be possible. Specify the port-channel parameter to set a channel group as the output destination for the static MAC address.

Related commands

vlan

18 VLAN

down-debounce

Sets the down-determination time of a VLAN interface when no more ports that can be used for relays exist in the VLAN.

Syntax

To set or change information:

down-debounce <seconds>

To delete information:

no down-debounce

Input mode

`(config-if)`

VLAN interface

Parameters

<seconds>

Sets the down-determination time (in seconds) of a VLAN interface when no more ports that can be used for relays exist in the VLAN.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 180

Default behavior

The VLAN interface goes down immediately when it is detected that there are no longer any ports that can be used for relaying the VLAN.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there are no more ports that can be used for relaying the VLAN in the following situations, the VLAN interface goes down immediately regardless of any setting by this command:

   - When no more ports belong to the VLAN
   - When the VLAN status is disabled by the "state" command

2. If the setting value is changed during the down-determination time of a VLAN interface, the VLAN interface goes down after the changed setting value elapses since the time when the value was changed.

3. If the setting value is deleted during the down-determination time of a VLAN interface, the interface

goes down when the value is deleted.

Related commands

None

interface vlan

Sets a VLAN interface. Entering this command switches to config-if mode, in which the IP address or other settings can be set for the relevant VLAN interface.

Syntax

To set information:

> interface vlan <vlan id>

To delete information:

> no interface vlan <vlan id>

Input mode

`(config)`

Parameters

<vlan id>

> Specifies a VLAN ID.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters". Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

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 VLAN ID which has not yet been set is specified for <vlan id>, a VLAN is created. Created VLANs are port VLANs. For a protocol VLAN or MAC VLAN, the VLAN must be created beforehand by using the "vlan" command.

2. If you set information for multiple VLAN interfaces, use the "interface range" command to set <vlan id list>. Note that an error will occur if you specify a VLAN ID which has not been set by using the "interface range" command, and a new VLAN will not be created.

3. Specifying no vlan for a VLAN that was created by the "interface vlan" command deletes the VLAN. Also, specifying the "no interface vlan" command for a VLAN that was created by the "vlan" command deletes the VLAN.

Related commands

vlan

l2protocol-tunnel eap

Enables the EAPOL forwarding function. The function is set for a device.

Syntax

To set information:

l2protocol-tunnel eap

To delete information:

no l2protocol-tunnel eap

Input mode

`(config)`

Parameters

None

Default behavior

The EAPOL forwarding function is invalid.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

l2protocol-tunnel lldp

Enables the LLDP forwarding function. The function is set for a device.

Syntax

To set information:

l2protocol-tunnel lldp

To delete information:

no l2protocol-tunnel lldp

Input mode

`(config)`

Parameters

None

Default behavior

The LLDP forwarding function is invalid.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

l2protocol-tunnel stp

Enables the BPDU forwarding function. The function is set for a device.

Syntax

To set information:

l2protocol-tunnel stp

To delete information:

no l2protocol-tunnel stp

Input mode

`(config)`

Parameters

None

Default behavior

The BPDU forwarding function is invalid.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

l2protocol-tunnel udld

Enables the UDLD forwarding function. The function is set for a device.

Syntax

To set information:

l2protocol-tunnel udld

To delete information:

no l2protocol-tunnel udld

Input mode

`(config)`

Parameters

None

Default behavior

The UDLD forwarding function is invalid.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

l2-isolation

Blocks Layer 2 forwarding within a VLAN. Only Layer 3 forwarding is permitted.

Syntax

To set information:

l2-isolation

To delete information:

no l2-isolation

Input mode

`(config)`

Parameters

None

Default behavior

Layer 2 forwarding is not blocked.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

mac-address

Sets the MAC address used to identify a MAC VLAN.

Syntax

To set information:

mac-address <mac>

To delete information:

no mac-address <mac>

Input mode

`(config-vlan) (MAC VLAN only)`

Parameters

<mac>

Specifies the MAC address setting for a MAC VLAN. This command can be set only when the applicable VLAN is a MAC VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to feff.ffff.ffff

   The lowest bit of the first byte (the multicast bit) must not be 1.

Default behavior

No MAC address is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. MAC addresses that are already assigned to another VLAN cannot be set. Delete the address, and then set it again.

2. If you specify a dynamically-set MAC address used for IEEE 802.1X, Web authentication, or MAC-based authentication, settings for those functions become invalid and settings for this command are enabled.

3. The maximum number of MAC addresses that can be set for a device is 1024.

Related commands

mac-based-vlan static-only

mac-based-vlan static-only

Allows only the "mac-address" command to register MAC addresses for MAC VLANs.

Syntax

To set information:

  mac-based-vlan static-only

To delete information:

  no mac-based-vlan static-only

Input mode

`(config)`

Parameters

None

Default behavior

If this command is not used, MAC addresses can be registered for MAC VLANs by using the "mac-address" command with the IEEE 802.1X, Web authentication, and MAC-based authentication functions.

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 used with any of the following functions:

   • IEEE802.1X

   • Web authentication

   • MAC-based authentication

Related commands

mac-address

name

Sets a VLAN name.

Syntax

To set or change information:

name \<string>

To delete information:

no name

Input mode

`(config-vlan)`

Parameters

\<string>

Sets a VLAN name. This parameter cannot be set if \<vlan id list> has been specified by using the "vlan" command.

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 "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The initial value is "VLANxxxx". Note that "xxxx" is a four-digit numeric string, including any leading zeros, that indicates a VLAN ID.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

protocol

Sets the protocol for identifying VLANs in protocol VLANs.

Syntax

To set information:

    protocol <protocol name>

To delete information:

    no protocol <protocol name>

Input mode

`(config-vlan)`

Parameters

<protocol name>

Specifies the name of the protocol in a protocol VLAN. This command can be set only when the applicable VLAN is a protocol VLAN. If you want to use multiple protocols in a single VLAN, specify this command as many times as the number of protocol names.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Protocol name set by the "vlan-protocol" command

Default behavior

No protocol is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To use a protocol VLAN with an IPv4 address or IPv6 address set, you must use this command to specify the applicable protocol.

Related commands

vlan-protocol

state

Sets the VLAN status.

Syntax

To set or change information:

　　state {suspend | active}

To delete information:

　　no state

Input mode

`(config-vlan)`

Parameters

{suspend | active}

　　suspend

　　　　Disables the VLAN status and stops the sending and receiving of all frames on the VLAN.

　　active

　　　　Sets the VLAN status to enable and starts the sending and receiving of all frames.

　　1. Default value when this parameter is omitted:

　　　This parameter cannot be omitted.

　　2. Range of values:

　　　None

Default behavior

The VLAN status is enable.

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 from the SNMP manager by using an SNMP SetRequest operation. If this command is set by using an SNMP SetRequest operation, the setting is applied to the configuration.

Related commands

None

switchport access

Sets access port information. The information you set is also applied to access VLANs of tunneling ports.

Syntax

To set or change information:

> switchport access vlan <vlan id>

To delete information:

> no switchport access vlan

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

vlan <vlan id>

> Sets an interface to the access port for the specified VLAN (access VLAN). The access VLAN for the tunneling port is also the specified 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

In non-VLAN tunneling mode, the access port for the default VLAN (VLAN ID = 1) is used. The default behavior in VLAN tunneling mode is for switch ports to not belong to any VLAN and for communication with VLANs to be disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. In non-VLAN tunneling mode, if an untagged frame or an access VLAN tagged frame is received, the frame is handled by the access VLAN. If a tagged frame of a VLAN other than an access VLAN is received, the frame is discarded.

2. In VLAN tunneling mode, frames are handled by access VLANs irrespective of whether they have a VLAN tag.

Related commands

switchport mode

vlan

switchport dot1q ethertype

Sets the TPID (Tag Protocol IDentifier) value that identifies VLAN frames on a port. This command is set when you connect to a network in which a non-standard TPID value is used.

Syntax

To set or change information:

> switchport dot1q ethertype <hex>

To delete information:

> no switchport dot1q ethertype

Input mode

`(config-if)`

> Ethernet interface

Parameters

<hex>

> Sets the TPID value of a VLAN tag which is assigned by a Switch. This command sets the default value for ports.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   Four-digit hexadecimal

Default behavior

When the "vlan-dot1q-ethertype" command is set, the setting value for the command is regarded as the TPID value. When the "vlan-dot1q-ethertype" command is not set, 0x8100 is regarded as the TPID value.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For ports specified by using this command, the value specified for vlan-dot1q-ethertype is not applied.
2. A maximum of four TPID values can be specified per device.

Related commands

None

switchport isolation

Configures the inter-port forwarding block function.

Syntax

To set information:

    switchport isolation interface <interface id list>

To change information:

    switchport isolation interface {<interface id list> | add <interface id list> | remove <interface id list>}

To delete information:

    no switchport isolation

Input mode

`(config-if)`

    Ethernet interface

Parameters

interface <interface id list>

    Specifies a list of physical ports from which forwarding is to be blocked. Forwarding from the specified ports to the interface is suppressed.

    1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

    2. Range of values:

        For details about how to specify <interface id list> and the specifiable range of values, see "Specifiable values for parameters".

interface add <interface id list>

    Adds ports forwarding from which is to be isolated to the list.

    1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

    2. Range of values:

        For details about how to specify <interface id list> and the specifiable range of values, see "Specifiable values for parameters".

interface remove <interface id list>

    Removes ports forwarding from which is isolated from the list.

    1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

    2. Range of values:

        For details about how to specify <interface id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

Forwarding between ports is not isolated.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The function for suppressing inter-port forwarding is entered from the line specified by interface of the "switchport isolation" command, and discards frames output from the port on which the command is set. To suppress forwarding on both ends, set the command on both lines.

2. If you use interface range to configure information for multiple interfaces, only one physical port can be specified.

   If you want to specify a list of ports for which to suppress forwarding, set the information for a single interface.

Related commands

None

switchport mac

Sets MAC VLAN port information.

Syntax

To set information:

switchport mac vlan <vlan id list>

switchport mac native vlan <vlan id>

switchport mac dot1q vlan <vlan id list>

To change information:

switchport mac {vlan <vlan id list> | vlan add <vlan id list> | vlan remove <vlan id list> | native vlan <vlan id> | dot1q vlan <vlan id list> | dot1q vlan add <vlan id list> | dot1q vlan remove <vlan id list>}

To delete information:

no switchport mac vlan

no switchport mac native vlan

no switchport mac dot1q vlan

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

vlan <vlan id list>

Specifies the list of valid MAC VLANs that applies to a switch port. When this value is changed, a list of the currently-valid MAC VLANs replaces the specified list.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

native vlan <vlan id>

Sets the VLAN that can receive frames with unregistered source MAC addresses. Frames can also be sent from the specified VLAN. Specifiable VLANs are port VLANs.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

dot1q vlan <vlan id list>

Sends the frames of the VLANs in the VLAN list set by using this parameter in the form of tagged frames. It is also possible to forward the tagged frames set by using this parameter. If a tagged frame is received by another VLAN, the frame is discarded.

VLANs configured by using the vlan parameter 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

vlan add <vlan id list>

Adds the currently-valid MAC VLANs for this port 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

vlan remove <vlan id list>

Removes the valid MAC VLANs for this port 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

dot1q vlan add <vlan id list>

Adds a VLAN able to forward tagged frames on the port to the VLAN list. VLANs configured by using the vlan parameter 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

dot1q vlan remove <vlan id list>

Removes a VLAN able to forward tagged frames on the port 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

None. If a MAC VLAN port has been set by using the "switchport mode" command with the mac-vlan parameter, and the "switchport mac" command has not been set, only the default VLAN is set. However, a MAC VLAN specified as a post-authentication VLAN by linking with the authentication function is available for communication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The MAC VLAN specified as a post-authentication VLAN by the authentication function is available for communication only when a valid MAC VLAN has not been set.

2. If valid MAC VLANs have been set, a MAC VLAN specified as a post-authentication VLAN by the authentication function is available for communication only when it matches a MAC VLAN that has been set. Therefore, if an authenticated terminal exists when a valid MAC VLAN has not been set, setting a valid MAC VLAN cancels the authentication of the terminal.

Related commands

switchport mode

vlan mac-based

switchport mode

Sets Layer 2 interface attributes.

Syntax

To set or change information:

switchport mode {access | trunk | protocol-vlan | mac-vlan | dot1q-tunnel | stack}

To delete information:

no switchport mode

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

{access | trunk | protocol-vlan | mac-vlan | dot1q-tunnel | stack}

Sets Layer 2 interface attributes.

access

Sets the applicable interface to access mode. When non-VLAN tunneling is used, untagged frames are sent or received in access mode. When VLAN tunneling is used, frames are sent or received in an access VLAN irrespective of whether the frames have a VLAN tag. Ports in access mode can be used only in a single VLAN.

trunk

Sets an interface to trunking mode. In trunking mode, untagged frames and tagged frames are sent and received.

protocol-vlan

Sets an interface to protocol VLAN mode. In protocol VLAN mode, untagged frames are sent and received. When a frame is received, the VLAN is determined by the protocol type of the frame. Tagged frames are discarded.

mac-vlan

Sets an interface to MAC VLAN mode. In MAC VLAN mode, untagged frames are sent and received. When a frame is received, the corresponding VLAN is determined from the source MAC address of the frame. Tagged frames are discarded. Note, however, that if the dot1q vlan parameter is set for the "switchport mac" command, tagged frames are sent and received.

If the vlan parameter is not set in the "switchport mac" command, a MAC VLAN specified as a post-authentication VLAN by linking with the authentication function is available for communication.

dot1q-tunnel

Sets an interface to tunneling mode. In tunneling mode, frames are sent and received on an access VLAN irrespective of whether the frames have a VLAN tag.

stack

Sets the applicable interface to stack port mode.

The following Ethernet interfaces can be set:

- interface fortygigabitethernet

- interface hundredgigabitethernet

1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

2. Range of values:

    None

Default behavior

access (access mode) is set.

stack (stack port mode) is set for interface fortygigabitethernet.

Impact on communication

If the interface is set to stack port mode, or is changed or deleted, the link of the interface goes down, which causes communication to stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If an interface is set to trunking mode, set allowed vlan by using the "switchport trunk" command. If an interface is set to trunking mode and allowed vlan is not set, all frames on the applicable port are discarded.

2. If an interface is set to protocol VLAN mode, use the "switchport protocol" command to set a protocol VLAN. If protocol VLAN is not set, the behavior of the applicable port is the same as in access mode.

3. If an interface is set to tunneling mode, use the "switchport access" command to set an access VLAN. Ports in tunneling mode are not automatically added to the default VLAN. Even when the default VLAN is used as the access VLAN, use the "switchport access" command to explicitly enable the access VLAN. If an access VLAN is not set, communication is not possible on tunneling ports.

4. If there are any ports on the device that are configured for tunneling mode, the entire device enters VLAN tunneling mode. As a result, the behavior of the ports in access mode is the same as in tunneling mode.

5. While the Switch is running in stack mode, if the interface is set to stack port mode, or if the mode is changed from stack port to any other mode, the link goes down.

6. The only available parameter is stack for interface fortygigabitethernet Ethernet interfaces.

7. For details on configurations that can be set when the stack port mode is set, see "Configuration Guide Vol. 1, 7.3.2 Stack port and stack link".

Related commands

None

switchport protocol

Sets protocol VLAN port information.

Syntax

To set information:

switchport protocol vlan <vlan id list>

switchport protocol native vlan <vlan id>

To change information:

switchport protocol {vlan <vlan id list> | vlan add <vlan id list> | vlan remove <vlan id list> | native vlan <vlan id>}

To delete information:

no switchport protocol vlan

no switchport protocol native vlan

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

vlan <vlan id list>

Sets the currently-valid protocol VLANs on the port. When this parameter is changed, the currently-valid protocol VLAN list replaces the specified list.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

native vlan <vlan id>

Sets a VLAN that sends and receives frames of a protocol that does not match the configuration. Specifiable VLANs are port VLANs.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

vlan add <vlan id list>

Adds a currently-valid protocol VLAN on the port 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 specify <vlan id list> and the specifiable range of values, see "Specifiable

values for parameters".

vlan remove <vlan id list>

Removes a currently-valid protocol VLAN on the port 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

None. If a protocol VLAN port has been set by using the "switchport mode protocol" command and the "switchport protocol" command is omitted, the default VLAN is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If no currently-valid protocol VLANs are set, the behavior of the port is the same as an access port.

2. If multiple protocol VLANs are set for a protocol VLAN port, be careful that you do not duplicate the protocols for the protocol VLAN.

Related commands

switchport mode

vlan protocol-based

vlan-protocol

switchport trunk

Sets trunk port information.

Syntax

To set information:

switchport trunk allowed vlan <vlan id list>

switchport trunk native vlan <vlan id>

To change information:

switchport trunk native vlan <vlan id>

switchport trunk allowed vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

To delete information:

no switchport trunk allowed vlan

no switchport trunk native vlan

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

native vlan <vlan id>

Sets the native VLAN (VLAN that sends and receives untagged frames). Specifiable VLANs are port VLANs. If the native VLAN is not set explicitly, the default VLAN becomes the native VLAN.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

allowed vlan <vlan id list>

Sets the VLANs that use a trunk port for sending and receiving frames.

The frames of VLANs that have not been specified are discarded.

To send and receive untagged frames, you must specify the native VLAN. If you do not set the native VLAN to allowed vlan, untagged frames are discarded.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

None. If trunking mode has been set by using the "switchport mode trunk" command and the command is omitted, communication is not possible.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If an interface is set to trunking mode, you must set allowed vlan. If allowed vlan is not set, no frames will be sent from or received at the applicable interface.

2. If you set the extended parameter with the "vxlan vlan-mapping mode" command, do not specify a VLAN for which the "vxlan-vni" command is set, for the native vlan parameter.

Related commands

switchport mode

vlan

switchport vlan mapping

Sets tag translation information entries.

Syntax

To set or change information:

switchport vlan mapping <vlan tag> <vlan id>

To delete information:

no switchport vlan mapping <vlan tag> <vlan id>

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

<vlan tag>

Specifies the VLAN tag value used in a LAN.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 4094

<vlan id>

Specifies the VLAN ID of a VLAN that handles frames.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

See "Specifiable values for parameters".

Default behavior

Tag translation is not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To enable tag translation, you must specify switchport vlan mapping enable.
2. Tag translation is enabled only when the applicable port is in trunking mode.

3. Do not specify the VLAN ID of the native VLAN for a VLAN tag or the VLAN ID.

4. Only VLAN tags for which switchport vlan mapping is set can be sent and received on the ports for which tag translation is enabled. For the ports that use tag translation, set the "switchport vlan mapping" command even if the VLAN tags to be sent or received match the VLAN IDs.

5. In a session using the 802.1Q tagging function of port mirroring, when setting tag translation for the port specified as a mirror port, the VLAN tag to be set with this command must be a value different from VLAN IDs used by the 802.1Q tagging function.

Related commands

switchport mode trunk

switchport trunk

switchport vlan mapping enable

switchport vlan mapping enable

Enables tag translation.

Syntax

To set information:

> switchport vlan mapping enable

To delete information:

> no switchport vlan mapping enable

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

None

Default behavior

Tag translation is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To enable tag translation, you must specify switchport vlan mapping.

2. Tag translation is enabled only when the applicable port is in trunking mode.

3. Only VLAN tags for which switchport vlan mapping is set can be sent and received on the ports for which tag translation is enabled. For the ports that use tag translation, set the "switchport vlan mapping" command even if the VLAN tags to be sent or received match the VLAN IDs.

Related commands

switchport mode

switchport trunk

switchport vlan mapping

up-debounce

Sets the up-determination time for a VLAN interface after the VLAN interface goes down until another port in the VLAN comes up again as a port that can be used for communication.

Syntax

To set or change information:

> up-debounce <seconds>

To delete information:

> no up-debounce

Input mode

`(config-if)`

> VLAN interface

Parameters

<seconds>

> Sets the up-determination time (in seconds) for a VLAN interface when another port in the VLAN comes up as a port that can be used for communication.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 3600

Default behavior

If a port in the VLAN comes up, and becomes available to restore communication, the VLAN interface comes up immediately.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. In the following situations, if a port in a VLAN comes up, and becomes available to restore communications, the VLAN interface comes up immediately, irrespective of the setting of this command:
   - When the device starts up
   - When the "restart vlan" operation command is executed
   - When the "copy" operation command is executed
   - When the VLAN status is changed from disable to enable by using the "state" command
2. For a VLAN interface, if the setting value is changed during the up-determination time, the VLAN in-

terface goes up after the changed setting value elapses since the time when the value was changed.

3. If the setting value is deleted during the up-determination time of a VLAN interface, the interface goes up when the value was deleted.

Related commands

None

vlan

Sets VLAN-related items.

Syntax

To set information:

    vlan <vlan id>

    vlan <vlan id list>

    vlan <vlan id> protocol-based

    vlan <vlan id list> protocol-based

    vlan <vlan id> mac-based

    vlan <vlan id list> mac-based

To delete information:

    no vlan <vlan id>

    no vlan <vlan id list>

Input mode

`(config)`

Parameters

<vlan id>

    Specifies a VLAN ID. When this command is entered, the mode switches to config-vlan mode.

    1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

    2. Range of values:

    See "Specifiable values for parameters". Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

<vlan id list>

    Specifies multiple VLAN IDs at one time. If you specify a VLAN ID for the first time, the applicable VLAN is newly created. When this command is entered, the mode switches to config-vlan mode.

    1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

    2. Range of values:

    For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters". Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

protocol-based

    Specify this parameter for a protocol VLAN.

    1. Default value when this parameter is omitted:

    The VLANs become port VLANs.

    2. Note on using this parameter:

- To specify protocol VLANs, you must specify protocol-based.

- This parameter cannot be specified for any VLAN which has already been created as a port VLAN or a MAC VLAN.

- This parameter and the VLAN tunneling function cannot be used at the same time.

mac-based

Specifies this parameter for MAC VLANs.

1. Default value when this parameter is omitted:

The VLANs become port VLANs.

2. Note on using this parameter:

- When specifying MAC VLANs, you must specify mac-based.

- This parameter cannot be specified for any VLAN which has already been created as a port VLAN or a protocol VLAN.

- This parameter and the VLAN tunneling function cannot be used at the same time.

Default behavior

No VLANs are configured.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. There is always a default VLAN (VLAN ID = 1). The configuration items for the VLAN are different from those of other normal VLANs.

2. If you specify a list by using <vlan id list>, you can configure multiple VLANs at the same time. Note, however, that if a list is specified (for multi-command mode) some commands cannot be used. For details, see the following table.

Table 18-1: Command availability in multi-command mode

No.	Command	Available in multi-command mode
1	state {suspend | active}	Y
2	name	N
3	protocol	Y
4	mac-address	N
5	vlan-mac	Y

Legend: Y: Can be used; N: Cannot be used

3. The default VLAN setting (VLAN ID=1) always exists in the configuration file and cannot be deleted. The initial state of the default VLAN is for all ports to be available as access ports.

4. The table below explains parameter items that can be set for the default VLAN, and behavior specific

to the default VLAN.

vlan command:

The following table applies to the "vlan" command.

Table 18-2: Handling default VLAN parameters

No.	Parameter	Whether specifiable by the user	Behavior specific to the default VLAN
1	<vlan id>	F (fixed value)	Set when the device starts up. Fixed at "1". Cannot be changed or deleted.
2	<vlan id list>	N	—
3	protocol-based	N	Port VLAN
4	mac-based	N	Port VLAN

Legend: F: Can be set as a fixed value; N: Cannot be set; —: Not applicable

config-vlan mode command:

The following table applies to the "config-vlan" mode command.

Table 18-3: Handling default VLAN parameters

No.	Command	Parameter	Whether specifiable by the user	Behavior specific to the default VLAN
1	state {suspend	active}	—	Y	—
2	name	<strings>	Y	—
3	protocol	<Protocol Name list>	N	—
4	mac-address	<MAC>	N	—
5	vlan-mac	—	Y	—

Legend: Y: Can be set; N: Cannot be set; —: Not applicable

5. When the "vlan" command is used to create a VLAN, information can be set for the VLAN interface by using the "interface vlan" command. For VLANs created by using the "vlan" command, use the "no interface vlan" command to delete information. For a VLAN created by using the "interface vlan" command, use the "no vlan" command to delete information.

Related commands

None

vlan-dot1q-ethertype

Sets the TPID for a VLAN tag.

Syntax

To set or change information:

vlan-dot1q-ethertype <hex>

To delete information:

no vlan-dot1q-ethertype

Input mode

`(config)`

Parameters

<hex>

Sets the TPID value of a VLAN tag which is assigned by a Switch. This command sets the default value of the entire device.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Four-digit hexadecimal

Default behavior

0x8100 is used as the TPID value. Note, however, that lines for which switchport dot1q ethertype is set, the setting value is used as the TPID value.

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-mac

Sets a MAC address to be used for each VLAN. When L3 forwarding is performed, if you change the MAC used by a Switch on a per-VLAN basis, this makes operation easier when you connect to a device that does not perform MAC address learning on a per-VLAN basis.

You do not have to set this command for VLANs for which L3 forwarding is not performed. Even if you set this command, the settings are not applied to the interfaces.

Syntax

To set information:

　　vlan-mac

To delete information:

　　no vlan-mac

Input mode

`(config-vlan)`

Parameters

None

Default behavior

Each device uses one MAC address.

Impact on communication

Setting the "vlan-mac" command changes the MAC address reported by a Switch when the Switch performs Layer 3 forwarding (including both frames originated by and frames addressed to and forwarded by the Switch) from the MAC address of the device to an individual MAC address for each VLAN (deleting the command is the reverse of setting it). Because of this, if this command is set for an already-operating VLAN, MAC addresses learned, using the ARP protocol, by neighboring Layer 3 devices (routers, Layer 3 switches, or terminals) no longer match the MAC address reported for each VLAN of the Switch. As a result, communication might be disabled temporarily.

When the change is applied

If vlan-mac-prefix has been set, the change takes effect immediately after the setting value is changed. If vlan-mac-prefix has not been set, no change takes effect until vlan-mac-prefix is set.

Notes

1. This command is valid only for VLAN interfaces for which IP addresses are set.

Related commands

vlan-mac-prefix

vlan-mac-prefix

Sets an individual MAC address prefix for each VLAN.

Syntax

To set or change information:

> vlan-mac-prefix <mac> <mask>

To delete information:

> no vlan-mac-prefix

Input mode

`(config)`

Parameters

<mac> <mask>

> Sets an individual MAC address to be used for each VLAN. Uses <mac> <mask> specified by using this command as the template, and automatically generates an MAC address for each VLAN by setting numbers corresponding to the VLAN in the lower order bits.

<mac>

> Specifies the MAC address prefix.

<mask>

> Specifies the mask for (pattern of high-order bits of) <mac> that are to be used unchanged.

> 1. Default value when this parameter is omitted:

> This parameter cannot be omitted.

> 2. Range of values:

> mask: Bit pattern with highest 8 to 34 bits turned on

> 3. Note on using this parameter:

> Multicast MAC addresses[#] cannot be set.

> #: An address in which the lowest bit of the first byte is 1.

Default behavior

The device MAC is used.

Impact on communication

If the "vlan-mac" command is set for a VLAN, when Layer 3 forwarding is performed by the VLAN (including both frames originated by, and frames addressed to and forwarded by, the Switch) the MAC address reported by the Switch for frames on that VLAN is changed. Because of this, the MAC addresses learned using ARP protocol by neighboring Layer 3 devices (routers, Layer 3 switches, or terminals) no longer match the MAC addresses reported for each VLAN of the Switch. As a result, communication might not be possible temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

vlan-mac

vlan-protocol

Sets the protocol name and protocol value for a protocol VLAN.

Syntax

To set or change information:

vlan-protocol <protocol name> [ethertype <hex>...] [llc <hex>...] [snap-ethertype <hex>...]

To delete information:

no vlan-protocol <protocol name>

Input mode

`(config)`

Parameters

<protocol name>

Sets the protocol name used for configuring the protocol VLAN.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

A string with 14 or fewer characters

ethertype <hex>

Specifies the EtherType value for an Ethernet V2-format frame.

1. Default value when this parameter is omitted:

None

2. Range of values:

Four-digit hexadecimal

3. Note on using this parameter:

EtherType values which have already been set by users cannot be specified.

llc <hex>

Specifies the LLC value (DSAP and SSAP) for 802.3-format frames.

1. Default value when this parameter is omitted:

None

2. Range of values:

Four-digit hexadecimal

3. Note on using this parameter:

LLC values which have already been set by users cannot be specified.

snap-ethertype <hex>

Specifies the EtherType value for an 802.3-format frame.

1. Default value when this parameter is omitted:

None

2. Range of values:

Four-digit hexadecimal

3. Note on using this parameter:

EtherType values which have already been set by users cannot be specified.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. Note, however, that for protocols that have not been specified by the "protocol" command for the protocol VLAN, the change is applied when the protocol name is specified by the "protocol" command.

Notes

None

Related commands

protocol

vlan-up-message

The "no vlan-up-message" command suppresses the sending of operation messages as well as linkUp and linkDown traps when the VLAN status is Up or Down.

Syntax

To set information:

vlan-up-message

To delete information:

vlan-up-message

Input mode

`(config)`

Parameters

None

Default behavior

Sends operation messages as well as linkUp and linkDown traps when the VLAN status is Up or Down.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The ifLinkUpDownTrapEnable value of the ifMIB group for VLAN is not affected by the setting of this command.

Related commands

None

19 VXLAN

[SL-L3A]

destination-ip

Sets a destination IPv4 address for a VXLAN tunnel.

Syntax

To set or change information:

destination-ip <ip address>

To delete information:

no destination-ip <ip address>

Input mode

`(config-if)`

VXLAN interface

Parameters

<ip address>

Specifies the IPv4 address.

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

None

Related commands

None

encapsulation dot1q

Sets a VLAN ID to logically multiplex Ethernet subinterfaces or port channel subinterfaces with the VLAN tag.

Syntax

To set or change information:

> encapsulation dot1q { <vlan id> | untagged }

To delete information:

> no encapsulation dot1q

Input mode

`(config-subif)`

> Ethernet subinterface, port channel subinterface

Parameters

{ <vlan id> | untagged }

> Sets a VLAN ID or specifies untagged.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot assign the same VLAN ID to another subinterface of the same port or port channel.

2. In a session using the 802.1Q tagging function of port mirroring, when setting a subinterface for the port specified as a mirror port, the VLAN ID to be set with this command must be a value different from VLAN IDs used by the 802.1Q tagging function.

Related commands

None

interface vxlan

Sets VXLAN VTEP information.

Entering this command switches to config-if mode, in which information about the relevant VXLAN interface can be set.

Syntax

To set information:

interface vxlan <vtep id>

To delete information:

no interface vxlan <vtep id>

Input mode

```
(config)
```

Parameters

<vtep id>

Specifies a VTEP ID.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

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

None

Related commands

None

member vni

Sets a VNI belonging to the VTEP.

Syntax

To set information:

member vni <vni list>

To change information:

member vni { <vni list> | add <vni list> | remove <vni list> }

To delete information:

no member vni

Input mode

`(config-if)`

VXLAN interface

Parameters

<vni list>

Sets a VNI belonging to the VTEP.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vni list> and the specifiable range of values, see "Specifiable values for parameters".

{ <vni list> | add <vni list> | remove <vni list> }

Modifies the specified VNI list. add specifies VNIs to be added to the specified VNI list, and remove specifies VNIs to be removed from the specified VNI list.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vni list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Different VTEPs cannot have the same VNI.

Related commands

None

source-interface

Sets a source interface to be added to VXLAN packets.

Syntax

To set or change information:

source-interface loopback <loopback id>

To delete information:

no source-interface loopback

Input mode

`(config-if)`

VXLAN interface

Parameters

loopback <loopback id>

Specifies a source interface.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

0 to 256

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

switchport

The "no switchport" command disables the Layer 2 interface.

Syntax

To set information:

    no switchport

To delete information:

    switchport

Input mode

`(config-if)`

    Ethernet interface, port channel interface

Parameters

None

Default behavior

Layer 2 interface settings are enabled.

Impact on communication

Communication stops because the link of the interface goes down.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Subinterfaces can be set after setting the "no switchport" command.
2. After setting the "no switchport" command, the existing switchport mode setting is deleted.
3. This setting cannot be deleted (that is, the "switchport" command cannot be set) while a subinterface is set.
4. This command cannot be set for interface fortygigabitethernet.
5. If this setting is deleted (that is, the "switchport" command is set), switchport mode is set to access mode.

Related commands

None

vxlan enable

Enables the VXLAN function.

Syntax

To set information:

vxlan enable

To delete information:

no vxlan enable

Input mode

`(config)`

Parameters

None

Default behavior

The VXLAN function is disabled.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

When the change is applied

When you set information, the new setting values take effect when the Switch is restarted. When you delete information, the change is applied immediately after setting values are changed.

Response messages

The following table shows the response messages for the "vxlan enable" command.

Table 19-1: Response messages for the vxlan enable command

Message	Description
After this command execute, please save configuration editing now in startup-config, and please reboot a device. Do you wish to continue ?(y/n):	After executing this command, save the edited configuration in the startup configuration file, and then restart the device. Enter "y" to execute the command. Enter "n" to cancel this operation.

Notes

1. After the VXLAN function is disabled, the device works with the following limitations until it is restarted.

   * The maximum number of multipath routes remains the same as when the VXLAN function is enabled.

   * The max number value of the VXLAN Layer2 Nexthop entry displayed by executing the "show system" operation command remains the same as when the VXLAN function is enabled.

   * Functions that cannot coexist with the VXLAN function cannot be used.

Related commands

None

vxlan pmtu

Enables the VXLAN PMTU function.

Syntax

To set or change information:

> vxlan pmtu <length>

To delete information:

> no vxlan pmtu

Input mode

`(config)`

Parameters

> Sets the MTU in octets for sending data to the VXLAN Network port. The MTU is the maximum length of the data section[#] for frames in Ethernet V2 format.
>
> #: For details on the frame format, see "Configuration Guide Vol. 1, 20.2.2 Frame format".
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   74 to 9216

Default behavior

The VXLAN PMTU function is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When using the VXLAN PMTU function, if the packet length is not changed on the host, communication will fail.

2. After editing a configuration with this command, confirm that the changes are reflected in the VXLAN PMTU display item of the "show vxlan" operation command before proceeding with another edit.

3. Even if <length> is set to 1279 octets or less, the size of a packet returned with ICMPv6 will be 1280 or 1284 octets.

Related commands

vxlan pmtu enable

vxlan pmtu enable

Enables the VXLAN PMTU function on the corresponding interface.

Syntax

To set or change information:

vxlan pmtu enable

To delete information:

no vxlan pmtu enable

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

The VXLAN PMTU function does not work on the interface.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Use the "vxlan pmtu" command to set the MTU length to less than that of the interface.

Related commands

vxlan pmtu

vxlan vlan-mapping mode

Sets the mode to increase the capacity limit when VLAN mapping is selected for the VNI mapping method.

Syntax

To set information:

vxlan vlan-mapping mode extended

To delete information:

no vxlan vlan-mapping mode

Input mode

`(config)`

Parameters

extended

Sets the mode to increase the capacity limit when VLAN mapping is selected.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The capacity limit is not increased when VLAN mapping is selected.

Impact on communication

When the value of this command is changed, the overlay (VXLAN) program automatically restarts. As a result, ports with VXLANs set are temporarily unable to send or receive data.

When the change is applied

The change is applied after the overlay (VXLAN) program restarts.

Response messages

The following table shows the response messages for the "vxlan vlan-mapping mode" command.

Table 19-2: Response messages for the vxlan vlan-mapping mode command

Message	Description
After this command execute, overlay program (vxland) restart automatically. Do you wish to continue ? (y/n):	After this command is executed, the overlay (VXLAN) program automatically restarts. Enter "y" to execute the command. Enter "n" to cancel this operation.

Notes

None

Related commands

None

vxlan-vni

Sets a VNI to be assigned to a subinterface or VLAN.

Syntax

To set or change information:

vxlan-vni <vni>

To delete information:

no vxlan-vni

Input mode

`(config-subif)`

Ethernet subinterface, port channel subinterface

`(config-vlan)`

Parameters

<vni>

Specifies a VNI.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 16777215

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 set the same VNI for a subinterface and VLAN. Note that the same VNI can be set for an Ethernet subinterface and port channel subinterface.

2. If this command is set for a VLAN, the VLAN can be used only with the VXLAN function, so the status of the VLAN will be disabled.

Related commands

None

20 Spanning Tree Protocols

instance

Sets VLANs belonging to Multiple Spanning Tree MST instances.

Syntax

To set or change information:

> instance <mst instance id> vlans <vlan range>

To delete information:

> no instance <mst instance id>

Input mode

`(config-mst)`

Parameters

<mst instance id>

> Sets an MST instance ID.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   0 to 4095

vlans <vlan range>

> Sets VLANs belonging to MST instances. One VLAN ID can be set. You can perform a batch setup of multiple VLAN IDs using hyphens (-) and commas (,).
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 4094
>
> 3. Note on using this parameter:
>
>   • All VLANs that do not belong to other MST instances participate in MST instance ID0.
>
>   • To configure the same MST region, the MST instance ID and the VLAN ID set by this parameter, as well as the values of the name parameter and the revision parameter, must match within the MST region.

Default behavior

All VLANs belong to MST instance ID0.

Impact on communication

When the "spanning-tree mode" command is used to set mst, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The "show" command does not display information about MST instance ID0.

2. When the Ring Protocol and Multiple Spanning Tree are used together, the VLAN IDs of VLANs specified by this command and the VLAN IDs specified by VLAN mapping for the Ring Protocol must match. Unmatched VLANs are put in the Blocking status.

Related commands

None

name

Sets a string to identify a Multiple Spanning Tree region.

Syntax

To set or change information:

name <name>

To delete information:

no name

Input mode

`(config-mst)`

Parameters

<name>

Sets the character string used to identify a region.

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 "■Arbitrary character string" in "Specifiable values for parameters".

3. Note on using this parameter:

To configure the same MST region, the values for this parameter and the revision parameter, as well as those of the MST instance ID and the VLAN ID set by the vlans parameter, must match within the MST region.

Default behavior

name is set to NULL.

Impact on communication

When the "spanning-tree mode" command is used to set mst, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

revision

Sets a revision number to identify a Multiple Spanning Tree region.

Syntax

To set or change information:

> revision <version>

To delete information:

> no revision

Input mode

`(config-mst)`

Parameters

<version>

> Sets the revision number to identify a region.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   0 to 65535
>
> 3. Note on using this parameter:
>
>   To configure the same MST region, the values for this parameter and the name parameter, as well as those of the MST instance ID and the VLAN ID set by the vlans parameter, must match within the MST region.

Default behavior

revision is set to 0.

Impact on communication

When the "spanning-tree mode" command is used to set mst, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree bpdufilter

Sets the BPDU filter function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

　　spanning-tree bpdufilter enable

To delete information:

　　no spanning-tree bpdufilter

Input mode

`(config-if)`

　　Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the BPDU guard function is disabled.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

None

spanning-tree bpduguard

Sets the BPDU guard function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree) for which the Port-Fast function has been set.

Syntax

To set or change information:

spanning-tree bpduguard { enable | disable }

To delete information:

no spanning-tree bpduguard

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

{ enable | disable }

Setting enable causes the BPDU guard function to take effect. Setting disable stops operation of the BPDU guard function.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The setting of the "spanning-tree portfast bpduguard default" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast default

spanning-tree portfast

spanning-tree portfast bpduguard default

spanning-tree cost

Sets the path cost of the applicable port. This command is applied to all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

>   spanning-tree cost <cost>

To delete information:

>   no spanning-tree cost

Input mode

`(config-if)`

>   Ethernet interface, port channel interface

Parameters

<cost>

>   Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.
>
>   1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
>   2. Range of values:
>
>   When short is set by the "spanning-tree pathcost method" command:
>
>   > 1 to 65535
>
>   When long is set by the "spanning-tree pathcost method" command:
>
>   > 1 to 200000000
>
>   3. Note on using this parameter:
>
>   Changing the path cost value might change the topology.

Default behavior

The method of applying the path cost is set by the "spanning-tree pathcost method" command.

1 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the "spanning-tree vlan cost" command, the "spanning-tree single cost" command, or the "spanning-tree mst cost" command is set, the value of the "spanning-tree cost" command is not applied.

2. When the "spanning-tree vlan pathcost method" command or the "spanning-tree single pathcost method" command is set, the value of the "spanning-tree cost" command is not applied.

3. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree pathcost method

spanning-tree vlan pathcost method

spanning-tree vlan cost

spanning-tree single pathcost method

spanning-tree single cost

spanning-tree mst cost

spanning-tree disable

Stops operation of the Spanning Tree function for all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

   spanning-tree disable

To delete information:

   no spanning-tree disable

Input mode

`(config)`

Parameters

None

Default behavior

The Spanning Tree Protocols are enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When a GSRP global configuration exists, the "no spanning-tree disable" command cannot be set.

Related commands

None

spanning-tree guard

Sets the guard function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree guard { loop | none | root }

To delete information:

no spanning-tree guard

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

{ loop | none | root }

If loop is set, the loop guard function is applied to the applicable ports. The loop guard function does not work for Multiple Spanning Tree.

If none is set, the guard function of the applicable port is stopped.

If root is set, the root guard function is applied to the applicable ports.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The setting of the "spanning-tree loopguard default" command is used.

Impact on communication

When the loop guard function is set for a port or channel group that does not receive BPDU, even after one such port comes UP, communications of the port might remain disabled, or it might take time until communication is enabled.

When the change is applied

When settings for the "spanning-tree portfast default" command or the "spanning-tree portfast" command are deleted, if you change the configuration stored in memory without setting the "spanning-tree portfast default" command or the "spanning-tree portfast" command, the changes take effect immediately after the change.

Notes

1. If the "spanning-tree portfast default" command or the "spanning-tree portfast" command are set, the changes are not applied.

2. After the loop guard function is set, if a device starts, a port (including a port in a channel group) comes up, a Spanning Tree program is restarted, or the Spanning Tree type is changed, then the loop guard function blocks the port. The loop guard function is not cleared until a BPDU is received.

3. If loop guard function is set while a port is on line, the function is not enabled. Loop guard function, set while a port is on line, is enabled when a BPDU reception timeout occurs.

4. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree loopguard default

spanning-tree link-type

Sets the link type of the applicable port. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree). If you want to change the high-speed topology when rapid-pvst or mst is set by the "spanning-tree mode" command, and rapid-pvst is set by the "spanning-tree vlan mode" command, the connection between bridges must be a Point-to-Point connection. If you want to change the high-speed topology when rapid-stp is set by the "spanning-tree single mode" command, the connection between bridges must be a Point-to-Point connection.

Syntax

To set or change information:

> spanning-tree link-type { point-to-point | shared }

To delete information:

> no spanning-tree link-type

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

{ point-to-point | shared }

> If point-to-point is set, Point-to-Point connection is used for the link type. If shared is set, a shared connection is used for the link type.

> 1. Default value when this parameter is omitted:

>   This parameter cannot be omitted.

> 2. Range of values:

>   None

Default behavior

point-to-point is used for a full-duplex port.

point-to-point is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The automatic-restoration function is enabled if point-to-point is set in STP compatibility mode. The automatic-restoration function does not work if shared is set in STP compatibility mode.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Pro-

tocol are used together.

Related commands

spanning-tree mode

spanning-tree vlan mode

spanning-tree single mode

spanning-tree loopguard default

Sets the loop guard function that is used by default. This command is valid for ports of all Spanning Tree Protocols (PVST+ and Single Spanning Tree).

Syntax

To set information:

    spanning-tree loopguard default

To delete information:

    no spanning-tree loopguard default

Input mode

`(config)`

Parameters

None

Default behavior

If the "spanning-tree guard" command is set, that setting is used. If the "spanning-tree guard" command is not set, this command has no effect.

Impact on communication

When loop guard function is set for a port or channel group that does not receive BPDU, even after one such port comes UP, communications of the port might remain disabled, or it might take time until communication is enabled.

When the change is applied

When settings for the "spanning-tree portfast default" command or the "spanning-tree portfast" command are deleted, if you change the configuration stored in memory without setting the "spanning-tree portfast default" command or the "spanning-tree portfast" command, the changes take effect immediately after the change.

Notes

1. If the "spanning-tree portfast default" command or the "spanning-tree portfast" command are set, the changes are not applied.

2. After the loop guard function is set, if a device starts, a port (including a port in a channel group) comes up, a Spanning Tree program is restarted, or the Spanning Tree type is changed, then the loop guard function blocks the port. The loop guard function is not cleared until a BPDU is received.

3. If loop guard function is set while a port is on line, the function is not enabled. Loop guard function, set while a port is on line, is enabled when a BPDU reception timeout occurs.

4. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree guard

spanning-tree mode

The following explains settings for the Spanning Tree running mode. This command applies to all Spanning Tree Protocols (PVST+ and Multiple Spanning Tree) other than Single Spanning Tree. If the "spanning-tree vlan mode" command is set in PVST+ running mode, the settings for that command are used.

Syntax

To set or change information:

    spanning-tree mode { pvst | rapid-pvst | mst }

To delete information:

    no spanning-tree mode

Input mode

`(config)`

Parameters

{ pvst | rapid-pvst | mst }

    Sets the protocol to be used. If the protocol is changed while using Spanning Tree, the Spanning Tree Protocol is re-initialized. If pvst is set, PVST+ is applied to all Spanning Tree Protocols. If rapid-pvst is set, rapid PVST+ is applied to all Spanning Tree Protocols. If mst is set, this defines all Spanning Tree Protocols as belonging to Multiple Spanning Tree. For Single Spanning Tree, pvst or rapid-pvst must be set.

    1. Default value when this parameter is omitted:

       This parameter cannot be omitted.

    2. Range of values:

       None

Default behavior

The configuration is explicitly set to spanning-tree mode pvst.

Impact on communication

Communication stops until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree link-type

spanning-tree mst configuration

Switches to config-mst mode in which you can set the information necessary for defining Multiple Spanning Tree regions. If this setting is deleted, all previously-set information for defining regions is deleted.

Syntax

To set information:

spanning-tree mst configuration

To delete information:

no spanning-tree mst configuration

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

None

Related commands

instance

name

revision

spanning-tree mst cost

Sets the path cost for the applicable Multiple Spanning Tree ports.

Syntax

To set or change information:

spanning-tree mst <mst instance id list> cost <cost>

To delete information:

no spanning-tree mst <mst instance id list> cost

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

<mst instance id list>

Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

0 to 4095

<cost>

Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 200000000

3. Note on using this parameter:

Changing the path cost value might change the topology.

Default behavior

The setting of the "spanning-tree cost" command is used.

1 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting information by using the "interface range" command, you cannot perform a batch setup of multiple MST instance IDs. Set one MST instance ID.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree cost

spanning-tree mst forward-time

Sets the time required for a Multiple Spanning Tree status transitions.

Syntax

To set or change information:

    spanning-tree mst forward-time <seconds>

To delete information:

    no spanning-tree mst forward-time

Input mode

`(config)`

Parameters

<seconds>

    Specifies the time in seconds required for the status of a port to change.

    For ports in stp-compatible mode, only listening and learning status can be maintained for the specified period of time. If a port is not in stp-compatible mode, only discarding and learning status are maintained for the specified period of time (note that this applies only when a timer causes a status transition).

    1. Default value when this parameter is omitted:

       This parameter cannot be omitted.

    2. Range of values:

       4 to 30

Default behavior

The time required for the status of a port to change is set to 15 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

spanning-tree mst hello-time

Sets the sending interval of BPDUs in Multiple Spanning Tree.

Syntax

To set or change information:

    spanning-tree mst hello-time <hello time>

To delete information:

    no spanning-tree mst hello-time

Input mode

`(config)`

Parameters

<hello time>

    Specifies the sending interval in seconds of BPDUs that are sent regularly from the Switch.

    1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

    2. Range of values:

        1 to 10

    3. Note on using this parameter:

        If you set 1 then this might result in a changeable topology.

Default behavior

The sending interval of BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree mst max-age

Sets the maximum valid time of BPDUs that are sent via Multiple Spanning Tree.

Syntax

To set or change information:

>   spanning-tree mst max-age <seconds>

To delete information:

>   no spanning-tree mst max-age

Input mode

`(config)`

Parameters

\<seconds\>

>   Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.
>
>   1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
>   2. Range of values:
>
>   6 to 40
>
>   3. Note on using this parameter:
>
>   If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 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

spanning-tree mst max-hops

Sets the maximum-number-of-hops count for BPDUs in Multiple Spanning Tree.

Syntax

To set or change information:

　　spanning-tree mst max-hops <hop number>

　　spanning-tree mst <mst instance id list> max-hops <hop number>

To delete information:

　　no spanning-tree mst max-hops

　　no spanning-tree mst <mst instance id list> max-hops

Input mode

`(config)`

Parameters

<mst instance id list>

　　Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

　　　1. Default value when this parameter is omitted:

　　　　All MST instances are selected.

　　　2. Range of values:

　　　　0 to 4095

<hop number>

　　Specifies the maximum-number-of-hops count for BPDUs sent by the Switch.

　　　1. Default value when this parameter is omitted:

　　　　20

　　　2. Range of values:

　　　　2 to 40

Default behavior

The maximum-number-of-hops count for BPDUs is set to 20.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree mst port-priority

Sets the priority of the applicable Multiple Spanning Tree ports for each MST instance.

Syntax

To set or change information:

spanning-tree mst <mst instance id list> port-priority <priority>

To delete information:

no spanning-tree mst <mst instance id list> port-priority

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

<mst instance id list>

Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

<priority>

Sets the port priority. Use a multiple of 16 as the port priority. The lower 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 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The setting of the "spanning-tree port-priority" command is used. If the "spanning-tree port-priority" command has not been set, the port priority is set to 128.

0 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting information by using the "interface range" command, you cannot perform a batch setup of multiple MST instance IDs. Set one MST instance ID.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree port-priority

spanning-tree mst root priority

Sets the bridge priority for each MST instance in Multiple Spanning Tree.

Syntax

To set or change information:

　　spanning-tree mst <mst instance id list> root priority <priority>

To delete information:

　　no spanning-tree mst <mst instance id list> root priority

Input mode

`(config)`

Parameters

<mst instance id list>

　　Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

　　1. Default value when this parameter is omitted:

　　　　This parameter cannot be omitted.

　　2. Range of values:

　　　　0 to 4095

<priority>

　　Sets the bridge priority. The lower the value, the higher the priority. Use a multiple of 4096 as the bridge priority.

　　1. Default value when this parameter is omitted:

　　　　This parameter cannot be omitted.

　　2. Range of values:

　　　　0 to 61440

　　3. Note on using this parameter:

　　　　Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

When both Spanning Tree Protocols and the Ring Protocol are used together, 0 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

None

spanning-tree mst transmission-limit

Sets the maximum number of BPDUs that can be sent during each hello-time interval for Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst transmission-limit <count>

To delete information:

no spanning-tree mst transmission-limit

Input mode

`(config)`

Parameters

<count>

Sets the maximum number of BPDUs that can be sent per hello-time interval.

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 BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree pathcost method

Sets whether to use 16-bit values or 32-bit values as the path cost of ports. This command does not apply to Multiple Spanning Tree but does apply to all other Spanning Tree Protocols (PVST+ and Single Spanning Tree).

When the "spanning-tree vlan pathcost method" command or the "spanning-tree single pathcost method" command is set, the value of the "spanning-tree pathcost method" command is not applied.

If setting of the "spanning-tree cost", "spanning-tree vlan cost", or "spanning-tree single cost" command is omitted, the following value is applied to the path cost according to the interface speed and the "spanning-tree pathcost method" command settings:

- When short is set by the "spanning-tree pathcost method" command:

  10 Mbit/s: 100

  100 Mbit/s: 19

  1 Gbit/s: 4

  10 Gbit/s: 2

  40 Gbit/s: 2

  100 Gbit/s: 2

- When long is set by the "spanning-tree pathcost method" command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  10 Gbit/s: 2000

  40 Gbit/s: 500

  100 Gbit/s: 200

Syntax

To set or change information:

  spanning-tree pathcost method { long | short }

To delete information:

  no spanning-tree pathcost method

Input mode

`(config)`

Parameters

{ long | short }

  If long is set, a 32-bit value is used. If short is set, a 16-bit value is used.

  1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

  2. Range of values:

    None

3. Note on using this parameter:

- The default value of the path cost changes.
- Changing the path cost value might change the topology.
- If the path cost value is set to 65536 or larger, you cannot change the parameter to short.

Default behavior

short is set by path cost mode.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When mst is set by the "spanning-tree mode" command, a 32-bit value is used for Multiple Spanning Tree. To set a value of 65536 or larger for the path cost using the "spanning-tree cost" command, you must set long for this command.

   You do not need to set this command before setting a path cost value using the "spanning-tree mst cost" command.

Related commands

spanning-tree cost

spanning-tree vlan pathcost method

spanning-tree vlan cost

spanning-tree single pathcost method

spanning-tree single cost

spanning-tree port-priority

Sets the port priority of the applicable ports. This command is applied to all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

> spanning-tree port-priority <priority>

To delete information:

> no spanning-tree port-priority

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

<priority>

> Sets the port priority. Use a multiple of 16 as the port priority. The lower 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 240
>
> 3. Note on using this parameter:
>
>   Changing the port priority might change the topology.

Default behavior

The settings of the "spanning-tree vlan port-priority", "spanning-tree single port-priority", or "spanning-tree mst port-priority" command are used. If the command described here has not been set, the port priority is set to 128.

0 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree vlan port-priority

spanning-tree single port-priority

spanning-tree mst port-priority

spanning-tree portfast

Sets the PortFast function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

    spanning-tree portfast [{ trunk | disable }]

To delete information:

    no spanning-tree portfast

Input mode

`(config-if)`

    Ethernet interface, port channel interface

Parameters

{ trunk | disable }

    If trunk is set, the PortFast function is applied to access, trunk, protocol, and MAC ports.

    If disable is set, the PortFast function stops.

    1. Default value when this parameter is omitted:

        The PortFast function, which is enabled on access, protocol, and MAC ports, is applied.

    2. Range of values:

        None

Default behavior

The setting of the "spanning-tree portfast default" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast default

spanning-tree portfast bpduguard default

Sets the BPDU guard function to be used by default. This command is valid for all ports (PVST+, Single Spanning Tree, and Multiple Spanning Tree) on which the PortFast function is set.

Syntax

To set information:

spanning-tree portfast bpduguard default

To delete information:

no spanning-tree portfast bpduguard default

Input mode

`(config)`

Parameters

None

Default behavior

If the "spanning-tree bpduguard" command is set, that setting is used. If the "spanning-tree bpduguard" command is not set, this command does not work.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast default

spanning-tree portfast

spanning-tree bpduguard

spanning-tree portfast default

Sets the PortFast function to be used by default. This command is valid on the access, protocol, and MAC ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

spanning-tree portfast default

To delete information:

no spanning-tree portfast default

Input mode

`(config)`

Parameters

None

Default behavior

If the "spanning-tree portfast" command has been set, that setting is used. If the "spanning-tree portfast" command has not been set, the "spanning-tree portfast" command does not work.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree portfast

spanning-tree loopguard default

spanning-tree guard

spanning-tree single

Starts calculation of the topology for Single Spanning Tree. If the Spanning Tree running mode is PVST+, VLAN 1 is treated as Single Spanning Tree after this command is executed.

Syntax

To set information:

    spanning-tree single

To delete information:

    no spanning-tree single

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. If VLAN 1 was subject to PVST+ before this command was executed, executing this command stops PVST+ for VLAN 1. Removing Single Spanning Tree causes PVST+ to be applied to VLAN 1. If the running mode is Multiple Spanning Tree, Single Spanning Tree does not work.

Related commands

spanning-tree mode

spanning-tree single cost

Sets the path cost for the applicable Single Spanning Tree ports.

Syntax

To set or change information:

 spanning-tree single cost <cost>

To delete information:

 no spanning-tree single cost

Input mode

`(config-if)`

 Ethernet interface, port channel interface

Parameters

<cost>

 Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.

 1. Default value when this parameter is omitted:

  This parameter cannot be omitted.

 2. Range of values:

  When short is set by the "spanning-tree pathcost method" or the "spanning-tree single pathcost method" command:

   1 to 65535

  When long is set by the "spanning-tree pathcost method" or the "spanning-tree single pathcost method" command:

   1 to 200000000

 3. Note on using this parameter:

  Changing the path cost value might change the topology.

Default behavior

The path cost is applied according to the setting of the "spanning-tree single pathcost method" command.

1 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

 1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Pro-

tocol are used together.

Related commands

spanning-tree cost

spanning-tree pathcost method

spanning-tree single pathcost method

spanning-tree single forward-time

Sets the time required for the status of Single Spanning Tree to change.

Syntax

To set or change information:

spanning-tree single forward-time <seconds>

To delete information:

no spanning-tree single forward-time

Input mode

`(config)`

Parameters

<seconds>

Specifies the time in seconds required for the status of a port to change.

If stp (802.1D) is set by the "spanning-tree single mode" command, the listening status and the learning status are maintained for the specified period of time. If rapid-stp (802.1w) is set by the "spanning-tree single mode" command, the discarding status and the learning status are maintained for the set period of time (note that this applies only when a timer causes the transition).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30

Default behavior

The time required for the status of a port to change is set to 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree single mode

spanning-tree single hello-time

Sets the sending interval of Single Spanning Tree BPDUs.

Syntax

To set or change information:

> spanning-tree single hello-time <hello time>

To delete information:

> no spanning-tree single hello-time

Input mode

`(config)`

Parameters

<hello time>

> Specifies the sending interval in seconds of BPDUs that are sent regularly from the Switch.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 10
>
> 3. Note on using this parameter:
>
>   If you set 1 then this might result in a changeable topology.

Default behavior

The sending interval of BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single max-age

Sets the maximum valid time of BPDUs that are sent via Single Spanning Tree.

Syntax

To set or change information:

    spanning-tree single max-age <seconds>

To delete information:

    no spanning-tree single max-age

Input mode

`(config)`

Parameters

<seconds>

    Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

    1. Default value when this parameter is omitted:

       This parameter cannot be omitted.

    2. Range of values:

       6 to 40

    3. Note on using this parameter:

       If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 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

spanning-tree single mode

Sets the Single Spanning Tree running mode.

Syntax

To set or change information:

spanning-tree single mode { stp | rapid-stp }

To delete information:

no spanning-tree single mode

Input mode

`(config)`

Parameters

{ stp | rapid-stp }

Sets the protocol to be used. If the protocol is changed while using Spanning Tree, the Spanning Tree Protocol is re-initialized. If stp is set, Spanning Tree mode is used. If rapid-stp is set, rapid Spanning Tree mode is used.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

stp is set for the Single Spanning Tree running mode.

Impact on communication

If the "spanning-tree single" command is set, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single pathcost method

Sets whether to use a 16-bit value or a 32-bit value as the path cost for Single Spanning Tree ports.

If the "spanning-tree single cost" command setting is omitted, the following values are applied to the path cost according to the interface speed and the setting of the "spanning-tree single pathcost method" command.

- If short is set by the "spanning-tree single pathcost method" command:

  10 Mbit/s: 100

  100 Mbit/s: 19

  1 Gbit/s: 4

  10 Gbit/s: 2

  40 Gbit/s: 2

  100 Gbit/s: 2

- If long is set by the "spanning-tree single pathcost method" command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  10 Gbit/s: 2000

  40 Gbit/s: 500

  100 Gbit/s: 200

Syntax

To set or change information:

spanning-tree single pathcost method { long | short }

To delete information:

no spanning-tree single pathcost method

Input mode

`(config)`

Parameters

{ long | short }

If long is set, a 32-bit value is used. If short is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

3. Note on using this parameter:

   - The default value of the path cost changes.
   - Changing the path cost value might change the topology.
   - When 65536 or a larger value is set for the path cost, you cannot change the parameter to short.

Default behavior

The setting of the "spanning-tree pathcost method" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree single port-priority

Sets the priority for applicable Single Spanning Tree ports.

Syntax

To set or change information:

    spanning-tree single port-priority <priority>

To delete information:

    no spanning-tree single port-priority

Input mode

`(config-if)`

    Ethernet interface, port channel interface

Parameters

<priority>

    Sets the port priority. Use a multiple of 16 as the port priority. The lower 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 240

    3. Note on using this parameter:

       Changing the port priority might change the topology.

Default behavior

The setting of the "spanning-tree port-priority" command is used. If the "spanning-tree port-priority" command has not been set, the port priority is set to 128.

0 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

None

spanning-tree single priority

Sets the bridge priority for Single Spanning Tree.

Syntax

To set or change information:

> spanning-tree single priority <priority>

To delete information:

> no spanning-tree single priority

Input mode

`(config)`

Parameters

<priority>

> Sets the bridge priority. The lower the value, the higher the priority. Use a multiple of 4096 as the bridge priority.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   0 to 61440
>
> 3. Note on using this parameter:
>
>   Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

When both Spanning Tree Protocols and the Ring Protocol are used together, 0 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

None

spanning-tree single transmission-limit

Sets the maximum number of BPDUs that can be sent during the hello-time interval for Single Spanning Tree.

Syntax

To set or change information:

 spanning-tree single transmission-limit <count>

To delete information:

 no spanning-tree single transmission-limit

Input mode

`(config)`

Parameters

<count>

 Sets the maximum number of BPDUs that can be sent per hello-time interval.

 This parameter is valid only when rapid-stp (802.1w) is set by the "spanning-tree single mode" command. If stp (802.1D) is set by the "spanning-tree single mode" command, the maximum number of BPDUs that can be sent per second is 3 (fixed) and the setting value of this command is ignored.

 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 BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree single mode

spanning-tree single hello-time

spanning-tree vlan

Configures PVST+. If the "no spanning-tree vlan" command is set after the "spanning-tree single" command has been set, the applicable VLAN works with Single Spanning Tree.

Syntax

To set information:

no spanning-tree vlan <vlan id list>

To delete information:

spanning-tree vlan <vlan id list>

Input mode

`(config)`

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

3. Note on using this command:

If the "spanning-tree single" command has been set, VLAN1 does not work in PVST+ mode.

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

vlan

spanning-tree vlan cost

Sets the path cost for the applicable PVST+ ports.

Syntax

To set or change information:

   spanning-tree vlan <vlan id list> cost <cost>

To delete information:

   no spanning-tree vlan <vlan id list> cost

Input mode

`(config-if)`

   Ethernet interface, port channel interface

Parameters

<vlan id list>

   Starts configuration of PVST+ for the set VLAN.

   1. Default value when this parameter is omitted:

      This parameter cannot be omitted.

   2. Range of values:

      For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

<cost>

   Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.

   1. Default value when this parameter is omitted:

      This parameter cannot be omitted.

   2. Range of values:

      When short is set by the "spanning-tree pathcost method" command or the "spanning-tree vlan pathcost method" command:

         1 to 65535

      When long is set by the "spanning-tree pathcost method" or the "spanning-tree vlan pathcost method" command:

         1 to 200000000

   3. Note on using this parameter:

      Changing the port priority might change the topology.

Default behavior

The method of applying the path cost is determined by the setting of the "spanning-tree vlan pathcost method" command.

1 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. <vlan id list> cannot be specified if the "interface range" command is used to set information.
2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree cost

spanning-tree pathcost method

spanning-tree vlan pathcost method

spanning-tree vlan forward-time

Sets the time required for PVST+ status transition.

Syntax

To set or change information:

> spanning-tree vlan <vlan id list> forward-time <seconds>

To delete information:

> no spanning-tree vlan <vlan id list> forward-time

Input mode

`(config)`

Parameters

<vlan id list>

> Starts configuration of PVST+ for the set VLAN.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

<seconds>

> Specifies the time in seconds required for the status of a port to change.
>
> If pvst (802.1D) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command, the listening status and the learning status are maintained for the set period of time.
>
> If rapid-pvst (802.1w) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command, the discarding status and the learning status are maintained for the set period of time (note that this applies only when the timer causes the transition).
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   4 to 30

Default behavior

The time required for the status of a port to change is set to 15 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

spanning-tree vlan hello-time

Sets the sending interval of PVST+ BPDUs.

Syntax

To set or change information:

> spanning-tree vlan <vlan id list> hello-time <hello time>

To delete information:

> no spanning-tree vlan <vlan id list> hello-time

Input mode

`(config)`

Parameters

<vlan id list>

> Starts configuration of PVST+ for the set VLAN.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

<hello time>

> Specifies the sending interval in seconds of BPDUs that are sent regularly from the Switch.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 10
>
> 3. Note on using this parameter:
>
>   If you set 1 then this might result in a changeable topology.

Default behavior

The sending interval of BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

spanning-tree vlan max-age

Sets the maximum valid time of BPDUs that are sent via PVST+.

Syntax

To set or change information:

    spanning-tree vlan <vlan id list> max-age <seconds>

To delete information:

    no spanning-tree vlan <vlan id list> max-age

Input mode

`(config)`

Parameters

<vlan id list>

    Starts configuration of PVST+ for the set VLAN.

      1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

      2. Range of values:

        For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

<seconds>

    Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

      1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

      2. Range of values:

        6 to 40

      3. Note on using this parameter:

        If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 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

spanning-tree vlan mode

Sets the PVST+ running mode.

Syntax

To set or change information:

> spanning-tree vlan <vlan id list> mode { pvst | rapid-pvst }

To delete information:

> no spanning-tree vlan <vlan id list> mode

Input mode

`(config)`

Parameters

<vlan id list>

> Starts configuration of PVST+ for the set VLAN.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

{ pvst | rapid-pvst }

> Sets the protocol to be used. If the protocol is changed while using Spanning Tree, the Spanning Tree Protocol is re-initialized. If pvst is set, PVST+ mode is used. If rapid-pvst is set, rapid PVST+ mode is used.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   None

Default behavior

The PVST+ running mode is set by the "spanning-tree mode" command.

Impact on communication

If pvst or rapid-pvst has been specified by the "spanning-tree mode" command, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mode

spanning-tree vlan pathcost method

Sets whether to use a 16-bit value or a 32-bit value as the path cost for a PVST+ port.

If the "spanning-tree vlan cost" command setting is omitted, the following values are applied to the path cost according to the interface speed and the "spanning-tree vlan pathcost method" command settings:

- When short is set by the "spanning-tree vlan pathcost method" command:

  10 Mbit/s: 100

  100 Mbit/s: 19

  1 Gbit/s: 4

  10 Gbit/s: 2

  40 Gbit/s: 2

  100 Gbit/s: 2

- When long is set by the "spanning-tree vlan pathcost method" command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  10 Gbit/s: 2000

  40 Gbit/s: 500

  100 Gbit/s: 200

Syntax

To set or change information:

spanning-tree vlan <vlan id list> pathcost method { long | short }

To delete information:

no spanning-tree vlan <vlan id list> pathcost method

Input mode

`(config)`

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

{ long | short }

If long is set, a 32-bit value is used. If short is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

3. Note on using this parameter:

- The default value of the path cost changes.

- Changing the path cost value might change the topology.

- When 65536 or a larger value is set for the path cost, you cannot change the parameter to short.

Default behavior

The setting of the "spanning-tree pathcost method" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree pathcost method

spanning-tree cost

spanning-tree vlan cost

spanning-tree vlan port-priority

Sets the priority for the applicable PVST+ ports.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> port-priority <priority>

To delete information:

no spanning-tree vlan <vlan id list> port-priority

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

<priority>

Sets the port priority. Use a multiple of 16 as the port priority. The lower 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 240

3. Note on using this parameter:

Changing the port priority might change the topology.

Default behavior

The setting of the "spanning-tree port-priority" command is used. If the "spanning-tree port-priority" command has not been set, the port priority is set to 128.

0 is applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. <vlan id list> cannot be specified if the "interface range" command is used to set information.

2. This command is not applied to a virtual link set when both Spanning Tree Protocols and the Ring Protocol are used together.

Related commands

spanning-tree port-priority

spanning-tree vlan priority

Sets the PVST+ bridge priority.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> priority <priority>

To delete information:

no spanning-tree vlan <vlan id list> priority

Input mode

`(config)`

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

<priority>

Sets the bridge priority. The lower the value, the higher the priority.

Use a multiple of 4096 as the bridge priority.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

0 to 61440

3. Note on using this parameter:

Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

When both Spanning Tree Protocols and the Ring Protocol are used together, 0 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

None

spanning-tree vlan transmission-limit

Sets the maximum number of BPDUs that can be sent within the PVST+ hello-time interval.

Syntax

To set or change information:

> spanning-tree vlan <vlan id list> transmission-limit <count>

To delete information:

> no spanning-tree vlan <vlan id list> transmission-limit

Input mode

`(config)`

Parameters

<vlan id list>

> Starts configuration of PVST+ for the set VLAN.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

<count>

> Sets the maximum number of BPDUs that can be sent per hello-time interval.
>
> This parameter is effective only when rapid-pvst (802.1w) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command. When pvst (802.1D) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command, the maximum number of BPDUs that can be sent per second is 3 (fixed) and the value set by this command is ignored.
>
> 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 BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mode

spanning-tree vlan mode

21 Ring Protocol

axrp

Set a ring ID. In addition, to collect information necessary for the Ring Protocol function, switches to config-axrp mode. A maximum of 24 ring IDs can be set for a Switch.

If this setting is removed, the ring information that is already set for ring IDs is deleted.

Syntax

To set information:

axrp <ring id>

To delete information:

no axrp <ring id>

Input mode

`(config)`

Parameters

<ring id>

Sets the ring ID.

The same ring ID must be specified for all devices belonging to the same ring. Specify a unique ring ID for each different ring in a network.

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

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When both the Ring Protocol and Spanning Tree Protocols are used or both the Ring Protocol and GSRP are used, or when the multi-fault monitoring function is used, a maximum of 8 ring IDs can be used.

2. In a stack configuration, when the Ring Protocol is used, configure two or more stack links to ensure sufficient bandwidth and redundancy.

Related commands

None

axrp virtual-link

Sets a virtual link ID used to identify the root bridge shared by a Spanning Tree Protocol and GSRP. Only one virtual link ID can be set for a Switch.

Syntax

To set or change information:

>   axrp virtual-link <link id> vlan <vlan id>

To delete information:

>   no axrp virtual-link <link id>

Input mode

`(config)`

Parameters

<link id>

>   Sets a virtual link ID.
>
>   1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
>   2. Range of values:
>
>   1 to 250

<vlan id>

>   Specifies a VLAN to be used for a virtual link.
>
>   1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
>   2. Range of values:
>
>   See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. VLANs that are used as control VLANs cannot be specified.

2. The multi-fault monitoring function cannot be used concurrently with a Spanning Tree Protocol or GSRP using a virtual link on the same device.

3. A node in a Spanning Tree Protocol can consist of a maximum of two switches (including this Switch)

that belong to the same Spanning Tree topology. Specify the same virtual link IDs for the two switches.

4. When the Ring Protocol is used with GSRP, set the same virtual link ID for the device that is used for GSRP.

Related commands

vlan

axrp vlan-mapping

Sets the VLAN mapping to be applied to a VLAN group and also the VLANs that participate in VLAN mapping.

Syntax

To set or change information:

> axrp vlan-mapping <mapping id> vlan <vlan id list>

To change information:

> axrp vlan-mapping <mapping id> {vlan <vlan id list> | vlan add <vlan id list> | vlan remove <vlan id list>}

To delete information:

> no axrp vlan-mapping <mapping id>

Input mode

`(config)`

Parameters

<mapping id>

> Specifies the VLAN mapping ID.
>
> > 1. Default value when this parameter is omitted:
> >
> >   This parameter cannot be omitted.
> >
> > 2. Range of values:
> >
> >   1 to 128

vlan <vlan id list>

> Sets the VLANs that participate in VLAN mapping. When specifying multiple VLANs, 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

vlan add <vlan id list>

> Specifies the VLANs to be added to the VLAN list you have configured.
>
> > 1. Default value when this parameter is omitted:
> >
> >   This parameter cannot be omitted.
> >
> > 2. Range of values:
> >
> >   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

vlan remove <vlan id list>

> Specifies the VLANs to be removed from the VLAN list you have configured.
>
> > 1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify multiple VLAN mappings for one VLAN.

2. You cannot specify a VLAN mapping for a VLAN that is used as the control VLAN.

3. You cannot specify a VLAN mapping for a VLAN that is used as the multi-fault monitoring VLAN.

4. When the Ring Protocol is used with PVST+, only one VLAN ID can be specified for a VLAN mapping. If you want to control multiple VLANs by using the Ring Protocol, set the remaining VLAN IDs for other VLAN mapping IDs, and then assign them to a VLAN group of the applicable ring ID.

5. When the Ring Protocol is used with Multiple Spanning Tree, the VLAN IDs specified by this command and the VLANs that belong to the MST instance must match. Unmatched VLANs are put in the Blocking status.

Related commands

vlan

axrp-primary-port

Sets the primary port on the master node.

If this command is set, the primary port is not assigned automatically on the master node, and the interface set by using this command serves as the primary port. The interfaces that can be specified are Ethernet interfaces and port channel interfaces.

Syntax

To set information:

> axrp-primary-port <ring id> vlan-group <group id>

To delete information:

> no axrp-primary-port <ring id> vlan-group <group id>

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

<ring id>

> Sets the ring ID.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 65535

vlan-group <group id>

> Specifies a VLAN group ID.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 2

Default behavior

The primary port is assigned automatically.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For an interface for which no ring port is set, if you enter this command, this will be ignored.

2. While the Ring Protocol is used, if you change or delete the primary port, this function is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.

3. When a Switch is on the following nodes, entering this command has no effect:

   - Transit node
   - Master node, which is an edge node for a shared link non-monitoring ring

4. You cannot specify an Ethernet interface that is part of a channel group as the primary port. Conversely, an Ethernet interface that is set as the primary port cannot be assigned to a channel group. Set the primary port to the port channel interface to which the applicable Ethernet interface belongs.

5. The ring ID must be associated with the same VLAN group as the primary port.

6. In a stack configuration, the primary port cannot be set for a port channel interface of a channel group in which ports of multiple member switches are registered.

Related commands

mode

axrp-ring-port

axrp-ring-port

Sets an interface to be used as the ring port for the Ring Protocol. The interfaces that can be set are Ethernet interfaces and port channel interfaces.

Syntax

To set or change information:

> axrp-ring-port <ring id> [{shared-edge | shared}]

To delete information:

> no axrp-ring-port <ring id>

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

<ring id>

> Sets the ring ID.
>
> > 1. Default value when this parameter is omitted:
> >
> > This parameter cannot be omitted.
> >
> > 2. Range of values:
> >
> > 1 to 65535

{shared-edge | shared}

> Specifies a ring port that configures a shared link.
>
> shared-edge
>
> > When a Switch serves as the edge node in a shared link non-monitoring ring, this parameter sets the ring port that will be a shared link.
> >
> > Only one port can be specified for the ring ID.
>
> shared
>
> > When a Switch serves as a transit node on a shared link, this parameter specifies the ring port that will be the shared link.
> >
> > Two ports must be specified to correspond with the ring ID.
>
> > 1. Default value when this parameter is omitted:
> >
> > The interface serves as a standard ring port.
> >
> > 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. Two ring ports can be specified as corresponding to one ring ID.

2. In a multi-ring configuration with shared links, when a Switch is already running as a master node in the neighboring ring, if a ring port with a shared-edge specified is set or deleted on a port which is used as the primary port, this function is disabled temporarily. As a result, a loop might occur depending on the network configuration (ring configuration) to which the function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.

3. An Ethernet interface that is part of a channel group cannot be specified as a ring port. Conversely, an Ethernet interface that is specified as a ring port cannot be part of a channel group. Set the ring port as the port channel interface to which the applicable Ethernet interface belongs.

4. If a Switch is specified as a master node, a primary port is assigned automatically to each VLAN group of registered ring ports. Note, however, that the interface specified by using the "axrp-primary-port" command takes priority and serves as the primary port.

5. If a shared port is not specified as a shared node, the Ring Protocol function will not work properly.

6. In a stack configuration, a ring port cannot be set for a port channel interface of a channel group in which ports of multiple member switches are registered. Also, only one ring port with the same ring ID can be set for a member switch. Set an interface of another member switch as the second ring port.

7. In a stack configuration, the shared-edge parameter cannot be specified.

Related commands

mode

axrp-primary-port

control-vlan

Sets the VLAN to be used as a control VLAN. You can use the VLAN specified by using this command to send and receive control frames that monitor the ring status.

Setting the forwarding-delay-time parameter for a transit node allows you to set the time required to transfer the status of the control VLAN to Forwarding during initialization. You can therefore adjust the time required before starting to monitor the status of received flush control frames on the transit node, to ensure that flush control frames sent by the master node are received.

Syntax

To set or change information:

> control-vlan <vlan id> [forwarding-delay-time <seconds>]

To delete information:

> no control-vlan

Input mode

`(config-axrp)`

Parameters

<vlan id>

> Specify the VLAN to be used as the control VLAN.
>
> 1. Default value when this parameter is omitted:
>
> This parameter cannot be omitted.
>
> 2. Range of values:
>
> See "Specifiable values for parameters".
>
> Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

forwarding-delay-time <seconds>

> Sets the time (in seconds) required before the status of the control VLAN changes to Forwarding when the transit node device is started or when the Ring Protocol program is restarted.
>
> 1. Default value when this parameter is omitted:
>
> The control VLAN transitions to Forwarding immediately after the ring port comes up.
>
> 2. Range of values:
>
> 1 to 65535
>
> 3. Note on using this parameter:
>
> To delete only this parameter, set control-vlan again with this parameter omitted. This operation is used to delete 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 a VLAN that is used as a control VLAN by another ring ID.

2. You cannot specify a VLAN that is used in a VLAN group.

3. For the control VLAN, you cannot specify a VLAN that is being used by the multi-fault monitoring VLAN.

4. While the Ring Protocol is operating, if you change or delete the control VLAN, this function is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.

5. The VLAN specified as a control VLAN cannot be used with Spanning Tree Protocols.

6. A VLAN used as a virtual link cannot be specified as a control VLAN.

7. forwarding-delay-time is enabled only when the running mode is transit node.

8. forwarding-delay-time takes effect when the following occurs:

   - The Switch is started (includes execution of the "reload" or "ppupdate" operation command).
   - Reflecting to configuration file operation (executing the "copy" operation command)
   - A Ring Protocol program is restarted (including execution of the "restart axrp" operation command).
   - A VLAN program is restarted (including execution of the "restart vlan" operation command).

Related commands

vlan

disable

Disables the Ring Protocol function.

Syntax

To set information:

    disable

To delete information:

    no disable

Input mode

`(config-axrp)`

Parameters

None

Default behavior

The Ring Protocol function is enabled.

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 entered while the Ring Protocol is operating, the Ring Protocol function is disabled. In this case, a loop might occur depending on a network configuration (ring configuration) to which the Ring Protocol function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.

Related commands

None

flush-request-count

Specifies the number of times the master node sends flush control frames, which clear the MAC address table, to the transit node in the ring if a ring failure occurs or when recovering from a failure.

Syntax

To set or change information:

> flush-request-count <count>

To delete information:

> no flush-request-count

Input mode

`(config-axrp)`

Parameters

<count>

> Specifies the number of times that flush control 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 flush control 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. The first-received flush control frame causes entries in the MAC address table on the transit node to be cleared. If a flush control frame is received while MAC address table entries are being cleared, the clearing of entries is aborted.

Related commands

None

flush-request-transmit vlan

Sets sending of flush control frames for neighboring rings to the devices in the neighboring ring configuration to clear the MAC address table when a ring failure occurs or the failure is corrected.

To configure this setting, see "Configuration Guide Vol. 1, 29.1.11 Configuring the flush control frames for neighboring rings".

Syntax

To set or change information:

> flush-request-transmit vlan <vlan id>

To delete information:

> no flush-request-transmit vlan

Input mode

`(config-axrp)`

Parameters

<vlan id>

> Specifies the ID of the VLAN to which flush control frames for neighboring rings are to be sent.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".

Default behavior

If this command is not specified, flush control frames for neighboring rings are not sent to the devices in the neighboring ring configuration.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set this command on the master node. The command's function is not enabled when the command is set on a transit node.

2. Make sure that the VLAN ID you specify is a VLAN ID specified in VLAN mapping.

   Do not use this VLAN ID for data transfer and use it only for sending flush control frames for neighboring rings.

Related commands

vlan

forwarding-shift-time

For a transit node, sets the reception hold time for flush control frames.

When the reception hold time passes, if no flush control frames are received, the status of a ring port changes from Blocking to Forwarding.

For a standalone master node, sets the hold time before the status switches to Forwarding when the secondary port is detected as up.

Syntax

To set or change information:

    forwarding-shift-time {<seconds> | infinity}

To delete information:

    no forwarding-shift-time

Input mode

`(config-axrp)`

Parameters

{<seconds> | infinity}

    For a transit node, specifies the hold time in seconds before a flush control frame is received.

    If you set "infinity", there is no limit on the hold time, and the status of the ring port on the transit node does not switch to Forwarding until a flush control frame is received.

    For a standalone master node, specifies the hold time in seconds before the status of the secondary port switches to Forwarding.

    If you set "infinity", there is no limit on the hold time, and the status of the secondary port does not switch to Forwarding even if the secondary port is detected as up.

    1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

    2. Range of values:

        1 to 65535 (seconds) or infinity

Default behavior

For a transit node, 10 seconds is used as the reception hold time for flush control frames.

For a standalone master node, 10 seconds is used as the hold time for the secondary port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the sending interval for health-check frames on the master node is longer than the reception hold time for flush control frames on the transit node, the status of the ring port on the transit node switches to Forwarding before the master node detects the normal status. This could produce a temporary loop.

   Set the hold time value based on the sending interval at which health-check frames are sent from the master node.

2. If the sending interval for health-check frames on a standalone master node is longer than the hold time before switching to Forwarding on the master node, the status of the secondary port switches to Forwarding before the master node detects the normal status. This could produce a temporary loop.

   Set the hold time value based on the sending interval at which health-check frames are sent from the master node.

3. This function does not work on the master node in a stack configuration.

Related commands

None

health-check holdtime

If the master node does not receive a periodic health-check frame sent by the master node itself or by shared edge nodes in a shared link non-monitoring ring, this specifies how long to wait before determining that a failure has occurred.

Syntax

To set or change information:

> health-check holdtime <milli seconds>

To delete information:

> no health-check holdtime

Input mode

```
(config-axrp)
```

Parameters

<milli seconds>

> Specifies the hold time in milliseconds until a health-check frame is received.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   500 to 300000
>
>   15 to 300000 [SL-L3A]

Default behavior

The reception hold time for health-check frames is set to 3000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For this command, set a value greater than the setting value of the "health-check interval" command. If you use this command to set a value equal to or smaller than the setting value of "health-check interval" command, a health-check timeout is detected.

2. When the hold time elapses, the master node determines that a failure has occurred, performs error processing, and then switches to the recovery monitoring status.

3. If the number of ring IDs is set to 9 or larger, make sure that you set the reception hold time for health-check frames to at least 3000 milliseconds.

Related commands

None

health-check interval

Sets the sending interval of health-check frames from a master node or from shared edge nodes in a shared link non-monitoring ring.

Syntax

To set or change information:

   health-check interval <milli seconds>

To delete information:

   no health-check interval

Input mode

`(config-axrp)`

Parameters

<milli seconds>

   Specifies the sending interval of health-check frames in milliseconds.

   1. Default value when this parameter is omitted:

      This parameter cannot be omitted.

   2. Range of values:

      200 to 60000

      5 to 60000 [SL-L3A]

Default behavior

The sending interval of health-check frames is 1000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set a value greater than the setting value of this command for the "health-check holdtime" command. If you set a value equal to or smaller than the setting value of this command for the "health-check hold-time" command, a health-check timeout is detected.

2. Set the same sending interval for health-check frames for the master nodes in the same ring and for the shared edge nodes in a shared link non-monitoring ring. If these values are different, failure detection will not work properly.

3. Set the number of ring IDs and the sending interval for health-check frames to specify the available setting values within the range shown in the following table.

Table 21-1: Available sending interval for health-check frames and the number of ring IDs

Health-check frame sending interval (milliseconds)	Number of ring IDs
5 to 9 [SL-L3A]	1 to 2
10 to 199 [SL-L3A]	1 to 4
200 to 999	1 to 8
1000 to 60000	1 to 24

Related commands

None

mac-clear-mode

Specifies MAC address table entries to be cleared when a ring failure occurs or is recovered.

Syntax

To set information:

    mac-clear-mode system

To delete information:

    no mac-clear-mode

Input mode

`(config-axrp)`

Parameters

system

Clears all entries in the MAC address table when a ring failure occurs or is recovered.

1. Default value when this parameter is omitted:

    This parameter cannot be omitted.

2. Range of values:

    None

Default behavior

MAC address table entries are cleared for each ring port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

mode

Sets the running mode of the Switch used for the ring.

In addition, if the ring configuration is a multi-ring configuration with shared links, sets the attributes of a ring configured by Switches, and the positioning of the Switches in the ring.

Syntax

To set or change information:

> mode {master | transit} [ring-attribute {rift-ring | rift-ring-edge <edge node id>}]

To delete information:

> no mode

Input mode

```
(config-axrp)
```

Parameters

{master | transit}

> Specifies the running mode.

> master

>> Serves as a master node.

> transit

>> Serves as a transit node.

> 1. Default value when this parameter is omitted:

>> This parameter cannot be omitted.

> 2. Range of values:

>> None

ring-attribute {rift-ring | rift-ring-edge <edge node id>}

> Specifies a shared link non-monitoring ring (a ring that does not monitor shared links) as the attributes of the ring in a multi-ring configuration with shared links, and specifies the positioning of a Switch in the ring.

> If you specify rift-ring-edge, you must specify the shared-edge parameter for the "axrp-ring-port" command.

> rift-ring

>> Serves as a node that is part of a shared link non-monitoring ring (but not an edge nodes). This parameter can be specified for the master node only.

> rift-ring-edge <edge node id>

>> Serves as a node (shared node) which is the edge node in a shared link non-monitoring ring. To differentiate between two edge nodes, specify an edge node ID (1 or 2) for each device.

> 1. Default value when this parameter is omitted:

>> For master nodes, the Switch serves as the master node for a shared link monitoring ring (ring that monitors shared links).

>> For transit nodes, the Switch serves as a shared link monitoring ring or a transit node of a shared

link non-monitoring ring.

2. Range of values:

Specify 1 or 2 for <edge node id>.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set only one master node device in a ring. If you specify multiple master node Switches, the Ring Protocol function will not work properly.

2. If you change or delete the mode while Ring Protocol is used, the function is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.

3. If you specify rift-ring-edge for the ring-attribute parameter, you must specify the shared-edge parameter for the "axrp-ring-port" command.

4. Specify different edge node IDs for each edge node in shared link non-monitoring rings within the same ring. If the setting is not correct, the ring function will not work properly.

5. Shared nodes do not work in a stack configuration.

Related commands

None

multi-fault-detection holdtime

This is used in a multi-ring configuration with shared links. This command sets the hold time before the shared nodes at both ends of a shared link determine that multiple faults occurred when the shared link monitoring rings did not receive any sent multi-fault monitoring frames.

Syntax

To set or change information:

> multi-fault-detection holdtime <milli seconds>

To delete information:

> no multi-fault-detection holdtime

Input mode

`(config-axrp)`

Parameters

<milli seconds>

> Specifies the hold time in milliseconds until a multi-fault monitoring frame is received.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1000 to 300000

Default behavior

The reception hold time for multi-fault monitoring frames is set to 6000 milliseconds.

Impact on communication

None

When the change is applied:

The change is applied immediately after setting values are changed.

Notes

1. The multi-fault monitoring function cannot be used concurrently with a Spanning Tree Protocol or GSRP using a virtual link on the same device.
2. For the "multi-fault-detection holdtime" command, set a value larger than the value of the "multi-fault-detection interval" command for the opposing node. If you specify a value equal to or less than the value specified for the "multi-fault-detection interval" command for the opposing node, multiple faults will be detected.
3. If the hold time elapses, the shared nodes determine that multiple faults occurred in the shared link monitoring rings, and perform a failure handling process.

Related commands

None

multi-fault-detection interval

This applies to a multi-ring configuration with shared links. This command sets the sending interval for multi-fault monitoring frames sent to the shared link monitoring rings from the shared nodes placed at both ends of a shared link.

Syntax

To set or change information:

multi-fault-detection interval <milli seconds>

To delete information:

no multi-fault-detection interval

Input mode

`(config-axrp)`

Parameters

<milli seconds>

Specifies the sending interval of multi-fault monitoring frames in milliseconds.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

500 to 60000

Default behavior

The sending interval of multi-fault monitoring frames is 2000 milliseconds.

Impact on communication

None

When the change is applied:

After the "multi-fault-detection mode" command is deleted, if you set it again, the setting will be applied to operation.

Notes

1. The multi-fault monitoring function cannot be used concurrently with a Spanning Tree Protocol or GSRP using a virtual link on the same device.

2. For the "multi-fault-detection interval" command, set a value less than the value of the "multi-fault-detection holdtime" command for the opposing node. If you specify a value greater than or equal to the value of the "multi-fault-detection holdtime" command, the opposing shared node will detect multiple faults.

Related commands

None

multi-fault-detection mode

Sets the multi-fault monitoring mode for shared link monitoring rings. Also sets the ring ID of the shared link non-monitoring ring used as the backup ring for switching the path in the route when multiple faults are detected.

Set this command for shared link monitoring rings in a multi-ring configuration with shared links.

Syntax

To set or change information:

> multi-fault-detection mode {monitor-enable backup-ring <ring id> | transport-only}

To delete information:

> no multi-fault-detection mode

Input mode

`(config-axrp)`

Parameters

{monitor-enable backup-ring <ring id> | transport-only}

> Specifies the monitoring mode for the multi-fault monitoring function.

> monitor-enable backup-ring <ring id>

>> Monitors sending and receiving of multi-fault monitoring frames. Set this parameter for the shared link monitoring rings in the shared edge node. In addition, specify the ring ID of the shared link non-monitoring ring used as the backup ring for switching the path in the route when multiple faults are detected.

> transport-only

>> Transfers multi-fault monitoring frames. Multi-fault monitoring is not performed.

> 1. Default value when this parameter is omitted:

>> This parameter cannot be omitted.

> 2. Range of values:

>> For <ring id>, the following range of values can be specified:

>> 1 to 65535

Default behavior

Multi-fault monitoring for shared link monitoring rings is not performed.

Impact on communication

None

When the change is applied:

The change is applied immediately after setting values are changed.

Notes

1. The multi-fault monitoring function cannot be used concurrently with a Spanning Tree Protocol or

GSRP using a virtual link on the same device.

2. The devices that monitor multiple faults must be the shared nodes at both ends of a shared link. If you enable the monitoring function (monitor-enable parameter) for a device other than a shared node, multi-fault monitoring cannot be performed correctly.

Related commands

None

multi-fault-detection vlan

Sets the VLAN for multi-fault monitoring. The VLAN specified for this command is used to send and receive control frames used for multi-fault monitoring.

Set this command for shared link monitoring rings in a multi-ring configuration with shared links.

Syntax

To set or change information:

> multi-fault-detection vlan <vlan id>

To delete information:

> no multi-fault-detection vlan

Input mode

`(config-axrp)`

Parameters

vlan <vlan id>

> Specifies a VLAN to be used for multi-fault monitoring.

> 1. Default value when this parameter is omitted:

>   This parameter cannot be omitted.

> 2. Range of values:

>   See "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this parameter.

Default behavior

Multi-fault monitoring for shared link monitoring rings is not performed.

Impact on communication

None

When the change is applied:

The change is applied immediately after setting values are changed.

Notes

1. The multi-fault monitoring function cannot be used concurrently with a Spanning Tree Protocol or GSRP using a virtual link on the same device.

2. You cannot specify a VLAN that is used as a multi-fault monitoring VLAN by another ring ID.

3. You cannot specify a VLAN that is used as a control VLAN as the multi-fault monitoring VLAN.

4. You cannot specify a VLAN that is used in VLAN mapping.

Related commands

None

name

Sets the name for identifying a ring.

Syntax

To set or change information:

    name <name>

To delete information:

    no name

Input mode

`(config-axrp)`

Parameters

<name>

    Sets the name for identifying a ring.

      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 "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

NULL 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

None

preempt-delay

Sets the suppression time between the detection of failure recovery by the master node and the start of path switchback.

When this command is set, if the master node detects failure recovery, the recovery process is not performed until the path switchback suppression time elapses.

Syntax

To set or change information:

preempt-delay { <seconds> | infinity }

To delete information:

no preempt-delay

Input mode

```
(config-axrp)
```

Parameters

{ <seconds> | infinity }

<seconds>

Specifies the path switchback suppression time in seconds.

infinity

The suppression time becomes unlimited and the master node does not start the recovery process until the "clear axrp preempt-delay" command is executed.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 3600 (seconds) or infinity

Default behavior

Path switchback is not suppressed.

Impact on communication

None

When the change is applied

If the ring status is normal, the value takes effect immediately after this command is set or changed. If the ring status is restoration suppression in a standalone configuration, or if a failure has occurred in the ring in a stack configuration, the setting will be applied next time.

If this command is deleted, the value takes effect immediately.

Notes

1. To set this function, set infinity for forwarding-shift-time of all transit nodes that configure a ring, or set a value greater than the suppression time for path switchback. If you specify a value smaller than the suppression time for path switchback, a loop might occur.

Related commands

None

vlan-group

Sets the VLAN group that will be used for the Ring Protocol and the mapping IDs of the VLANs participating in the VLAN groups.

A maximum of two VLAN groups can be set for a ring. In addition, by creating two VLAN groups, loads can be balanced between the two VLANs.

Syntax

To set or change information:

> vlan-group <group id> vlan-mapping <mapping id list>

To delete information:

> no vlan-group <group id>

Input mode

`(config-axrp)`

Parameters

<group id>

> Specifies the VLAN group ID that will be used for the Ring Protocol.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 2

vlan-mapping <mapping id list>

> Specifies the mapping IDs of the VLANs participating in a VLAN group. One VLAN mapping ID can be set. You can perform a batch setup of multiple VLAN mapping IDs using hyphens (-) and commas (,).
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 128

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 same VLAN mapping is assigned to VLAN groups in different rings, these rings cannot share the same port as a ring port. Note, however, that it is possible to share the same ring port if it is a shared link ring port (a ring port for which shared or shared-edge is specified).

2. If a Switch is specified as a master node, a primary port is assigned automatically to each VLAN group of registered ring ports. If the "axrp-primary-port" command is already entered, the specified interface has priority and set as the primary port.

Related commands

axrp vlan-mapping

22 IGMP snooping

ip igmp snooping (global)

Suppresses the IGMP snooping function on a Switch.

Syntax

To set information:

> no ip igmp snooping

To delete information:

> ip igmp snooping

Input mode

`(config)`

Parameters

None

Default behavior

The IGMP snooping function is enabled on a Switch.

Impact on communication

The IGMP snooping function stops.

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If the "no ip igmp snooping" command is set, IGMP snooping is disabled on the Switch. Therefore, setting the "ip igmp snooping" command on a VLAN interface does not enable IGMP snooping on the interface.

Related commands

None

ip igmp snooping (VLAN interface)

Enables the IGMP snooping function on a VLAN interface.

Syntax

To set information:

    ip igmp snooping

To delete information:

    no ip igmp snooping

Input mode

`(config-if)`

    VLAN interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. To concurrently use IGMP snooping and the IP multicast routing function on the Switch, make sure that you set the "swrt_multicast_table" command.

   When using IGMP snooping and the IPv4 multicast routing function at the same time, make sure that you use IPv4 multicast routing function on the corresponding VLAN. The IGMP snooping function is disabled for VLANs if the IPv4 multicast routing function is not used.

2. If the "no ip igmp snooping" command is set in global configuration mode, IGMP snooping is disabled on the Switch. Therefore, setting this command does not enable IGMP snooping on the interface.

3. This command cannot be set for a VLAN with 7 or more IPv4 addresses set.

Related commands

None

ip igmp snooping fast-leave

Immediately stops multicast communication to the applicable port if IGMP Leave and IGMPv3 Report (leave request) messages are received on a VLAN interface.

Syntax

To set information:

ip igmp snooping fast-leave

To delete information:

no ip igmp snooping fast-leave

Input mode

`(config-if)`

VLAN interface

Parameters

None

Default behavior

If IGMP Leave and IGMPv3 Report (leave request) messages are received, make sure there are no members from the same multicast group on the applicable port, and then stop multicast communication. Multicast communication will continue (for a default value of three seconds) for the check process after IGMP Leave and IGMPv3 Report (leave request) messages are received.

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. Immediately stops multicast communication to the applicable port if you set this command and receive IGMP Leave and IGMPv3 Report (leave request) messages. For this reason, if there are members from the same multicast group on the applicable port, multicast communication to the applicable members stops temporarily. In this case, multicast communication is restarted when an IGMP Report (membership request) message is received again from the applicable member.

Related commands

None

ip igmp snooping mrouter

Specifies a multicast router port on a VLAN interface.

Syntax

To set information:

ip igmp snooping mrouter interface <interface type> <interface number>

To delete information:

no ip igmp snooping mrouter interface <interface type> <interface number>

Input mode

`(config-if)`

VLAN interface

Parameters

<interface type> <interface number>

Specifies an interface for which a multicast router port is set.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

- Ethernet interface
- Port channel interface

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If ip igmp snooping is not specified for the applicable interface, this function does not work.

2. Some of ports with port channel interfaces set cannot be specified as multicast router ports. If you do so, the applicable port becomes invalid.

Related commands

ip igmp snooping

ip igmp snooping querier

Enables the IGMP querier function on a VLAN interface.

Syntax

To set information:

ip igmp snooping querier

To delete information:

no ip igmp snooping querier

Input mode

`(config-if)`

VLAN interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If ip igmp snooping is not specified for the applicable interface or the IP address is not set, the querier function does not work.

Related commands

ip igmp snooping

ip address

23 MLD snooping

ipv6 mld snooping (global)

Suppresses the MLD snooping function on a Switch.

Syntax

To set information:

    no ipv6 mld snooping

To delete information:

    ipv6 mld snooping

Input mode

`(config)`

Parameters

None

Default behavior

The MLD snooping function is enabled on a Switch.

Impact on communication

The MLD snooping function stops.

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If no ipv6 mld snooping is set, MLD snooping is disabled on the Switch. Therefore, setting the "ipv6 mld snooping" command on a VLAN interface does not enable MLD snooping on the interface.

Related commands

None

ipv6 mld snooping (VLAN interface)

Enables the MLD snooping function on a VLAN interface.

Syntax

To set information:

> ipv6 mld snooping

To delete information:

> no ipv6 mld snooping

Input mode

`(config-if)`

> VLAN interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. To concurrently use MLD snooping and the IP multicast routing function on the Switch, make sure that you set the "swrt_multicast_table" command. The following describes functional situations when the "swrt_multicast_table" command is set:

   - If a pattern that allocates resources to IPv6 routing is set for the "swrt_table_resource" command, make sure that the IPv6 multicast routing function is used for the target VLANs. The MLD snooping function is disabled for VLANs if the IPv6 multicast routing function is not used.

   - If a pattern that allocates resources only to IPv4 routing is set for the "swrt_table_resource" command, the MLD snooping function is enabled for the target VLANs.

2. If the "no ipv6 mld snooping" command is set in global configuration mode, MLD snooping is disabled on the Switch. Therefore, setting this command does not enable MLD snooping on the interface.

Related commands

None

ipv6 mld snooping mrouter

Specifies a multicast router port on a VLAN interface.

Syntax

To set information:

> ipv6 mld snooping mrouter interface <interface type> <interface number>

To delete information:

> no ipv6 mld snooping mrouter interface <interface type> <interface number>

Input mode

`(config-if)`

> VLAN interface

Parameters

<interface type> <interface number>

> Specifies an interface for which a multicast router port is set.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".
>
>   - Ethernet interface
>   - Port channel interface

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If ipv6 mld snooping is not specified for the applicable interface, this function does not work.
2. Some of ports with port channel interfaces set cannot be specified as multicast router ports. If you do so, the applicable port becomes invalid.

Related commands

ipv6 mld snooping

ipv6 mld snooping querier

Enables the MLD querier function on a VLAN interface.

Syntax

To set information:

    ipv6 mld snooping querier

To delete information:

    no ipv6 mld snooping querier

Input mode

`(config-if)`

    VLAN interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If ipv6 mld snooping is not specified for the applicable interface or the IP address is not set, the querier function does not work.

Related commands

ipv6 mld snooping

ipv6 address

24 Flow Detection Modes/Flow Performance

flow action-change arp-discard-class

Changes the queuing priority of ARP broadcast frames for the device.

Setting this command changes the queuing priority of ARP broadcast frames from 3 to 2.

Because this command is used to change the queuing priority behavior, make sure you set this command during the first stage of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set information:

   flow action-change arp-discard-class

To delete information:

   no flow action-change arp-discard-class

Input mode

`(config)`

Parameters

None

Default behavior

The queuing priority of ARP broadcast frames is not changed.

Impact on communication

Enabling this command may cause ARP broadcast frames (ARP Request) to be discarded.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

flow action-change arp-reply-cos

Changes the CoS value of ARP reply frames received by the Switch and whose destination MAC address is the broadcast address from 5 to 0.

Because this command is used to change the priority behavior in the device, make sure you set this command during the first stage of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set information:

   flow action-change arp-reply-cos

To delete information:

   no flow action-change arp-reply-cos

Input mode

`(config)`

Parameters

None

Default behavior

The CoS value of ARP reply broadcast frames received by the Switch is not changed.

Impact on communication

Enabling this command may cause ARP reply broadcast frames received by the Switch to be discarded.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

flow action-change cos

Changes the QoS priority determination behavior for the device.

When the stack function is disabled, by setting this command, frames sent to the Switch become subject to priority determination.

Because this command is used to change the priority determination behavior, make sure you set this command during the first stage 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, the behavior as described in Default behavior is enabled.

Syntax

To set information:

    flow action-change cos

To delete information:

    no flow action-change cos

Input mode

`(config)`

Parameters

None

Default behavior

The priority determination behavior is not changed when the stack function is disabled. Only frames forwarded by the Switch become subject to priority determination.

When the stack function is enabled, only frames forwarded by the Switch and frames sent to the Switch are subject to priority determination.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To change the priority determination behavior, you need to delete all QoS flow detection conditions and performance information entries applied to the interface.

Related commands

ip qos-flow-group

ipv6 qos-flow-group

mac qos-flow-group

flow detection mode

Sets the flow detection mode for the filters and QoS function for the receiving-side interface.

This command changes the allocation pattern for the maximum number of entries in a hardware table.

By changing the allocation pattern according to the operating mode, you can collect hardware resource information in the necessary tables and use it.

Because this command is used to set the basic conditions under which the hardware runs, make sure you set this command during the first stage of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set or change information:

> flow detection mode {<layer3 mode> | <custom mode>}

To delete information:

> no flow detection mode

Input mode

`(config)`

Parameters

<layer3 mode> parameter

{layer3-1 | layer3-2 | layer3-6 | layer3-dhcp-1 | layer3-mirror-1 | layer3-mirror-2 | layer3-mirror-3 | layer3-mirror-4 | layer3-mirror-5 | layer3-suppress-1 | layer3-suppress-2 | layer3-suppress-dhcp-1 | layer3-suppress-mirror-1 | layer3-suppress-mirror-2}

> Specifies a flow detection mode for which a hardware table allocation is predefined.
>
>   1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
>   2. Range of values:
>
>   None
>
> The following table describes the commands applicable to the flow detection modes.

Table 24-1: Commands applicable to flow detection mode (filter)

Flow detection mode	Applicable command					
	mac access-group		ip access-group		ipv6 traffic-filter	
	in	in-mirror	in	in-mirror	in	in-mirror
layer3-1	Y	N	Y	N	N	N
layer3-2	N	N	Y	N	N	N
layer3-6	N	N	Y	N	Y	N
layer3-dhcp-1	N	N	Y	N	N	N
layer3-mirror-1	Y	Y	Y	Y	N	N

Flow detection mode	Applicable command					
	mac access-group		ip access-group		ipv6 traffic-filter	
	in	in-mirror	in	in-mirror	in	in-mirror
layer3-mirror-2	N	N	Y	Y	N	N
layer3-mirror-3	N	Y	Y	Y	Y	N
layer3-mirror-4	N	N	Y	N	Y	Y
layer3-mirror-5	N	Y	Y	Y	Y	Y
layer3-suppress-1	Y	N	Y	N	N	N
layer3-suppress-2	N	N	Y	N	Y	N
layer3-suppress-dhcp-1	N	N	Y	N	N	N
layer3-suppress-mirror-1	Y	Y	Y	Y	N	N
layer3-suppress-mirror-2	N	N	Y	Y	Y	Y

Legend: Y: Can be set; N: Cannot be set

Table 24-2: Commands applicable to flow detection mode (QoS)

Flow detection mode	Applicable command		
	mac qos-flow-group	ip qos-flow-group	ipv6 qos-flow-group
	in	in	in
layer3-1	Y	Y	N
layer3-2	N	Y	N
layer3-6	N	Y	Y
layer3-dhcp-1	N	Y	N
layer3-mirror-1	Y	Y	N
layer3-mirror-2	N	Y	N
layer3-mirror-3	N	Y	Y
layer3-mirror-4	N	Y	Y
layer3-mirror-5	N	Y	N
layer3-suppress-1	Y	Y	N
layer3-suppress-2	N	Y	Y
layer3-suppress-dhcp-1	N	Y	N
layer3-suppress-mirror-1	Y	Y	N
layer3-suppress-mirror-2	N	N	N

Legend: Y: Can be set; N: Cannot be set

For each flow detection mode, see "Configuration Guide Vol. 2, 1.1.3 Receiving-side flow detection mode" and "Configuration Guide Vol. 2, 3.1.1 Receiving-side flow detection mode".

<custom mode> parameter

custom { {1 <single entry block> 2 <single entry block> | 1-2 <double entry block>} {3 <single entry block> 4 <single entry block> | 3-4 <double entry block>} {5 <single entry block> 6 <single entry block> | 5-6 <double entry block>} {7 <single entry block> 8 <single entry block> | 7-8 <double entry block>} | suppress {1 <single entry block> 2 <single entry block> | 1-2 <double entry block>} {3 <single entry block> 4 <single entry block> | 3-4 <double entry block>} {7 <single entry block> 8 <single entry block> | 7-8 <double entry block>} }

Specifies allocation of flow detection conditions for flow detection modes. The hardware table in which flow detection conditions can be specified has entry blocks 1 to 8, and you can freely specify allocation pattern.

If you specify the same flow detection condition for multiple entry blocks, specify it using consecutive entry blocks.

If suppress is specified, entry blocks 5 and 6 in the hardware table cannot be specified, resulting in IP unset VLAN suppression mode.

- <single entry block>

mac-filter

Specifies a filter for MAC conditions.

Filter entries for MAC conditions can be specified with the in parameter of the "mac access-group" command.

mac-pbm

Specifies policy-based mirroring for MAC conditions.

Policy-based mirroring entries for MAC conditions can be specified with the in-mirror parameter of the "mac access-group" command.

mac-qos

Specifies QoS for MAC conditions.

QoS entries for MAC conditions can be specified with the in parameter of the "mac qos-flow-group" command.

ip-filter

Specifies a filter for IPv4 packet conditions.

Filter entries for IPv4 packets can be specified with the in parameter of the "ip access-group" command.

ip-pbm

Specifies policy-based mirroring for IPv4 packet conditions.

Policy-based mirroring entries for IPv4 packets can be specified with the in-mirror parameter of the "ip access-group" command.

ip-qos

Specifies QoS for IPv4 packet conditions.

QoS entries for IPv4 packet conditions can be specified with the in parameter of the "ip qos-flow-group" command.

dhcp-filter

Specifies a terminal filter of DHCP snooping.

A terminal filter of DHCP snooping can be specified with the "ip verify source" command.

- <double entry block>

ipv6-filter

Specifies a filter for IPv6 packet conditions.

Filter entries for IPv6 packet conditions can be specified with the in parameter of the "ipv6 traffic-filter" command.

ipv6-pbm

Specifies policy-based mirroring for IPv6 packet conditions.

Policy-based mirroring entries for IPv6 packet conditions can be specified with the in-mirror parameter of the "ipv6 traffic-filter" command.

ipv6-qos

Specifies QoS for IPv6 packet conditions.

QoS entries for IPv6 packet conditions can be specified with the in parameter of the "ipv6 qos-flow-group" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The flow detection mode is set to layer3-2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip access-group

ipv6 traffic-filter

mac access-group

ip qos-flow-group

ipv6 qos-flow-group

mac qos-flow-group

policy-list

policy-list default-init-interval

policy-list default-aging-interval

flow detection out mode

Sets the flow detection mode for the filter function for the sending-side interface.

This command changes the allocation pattern for the maximum number of entries in a hardware table.

By changing the allocation pattern according to the operating mode, you can collect hardware resource information in the necessary tables and use it.

Because this command is used to set the basic conditions under which the hardware runs, make sure you set this command during the first stage of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set or change information:

flow detection out mode {layer3-1-out | layer3-2-out}

To delete information:

no flow detection out mode

Input mode

`(config)`

Parameters

{layer3-1-out | layer3-2-out}

Specifies the sending-side flow detection mode.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

The following table describes the commands applicable to the sending-side flow detection modes.

Table 24-3: Commands applicable to sending-side flow detection mode

Sending-side flow detection mode	Applicable command		
	Filters		
	mac access-group	ip access-group	ipv6 traffic-filter
layer3-1-out	N	Y	N
layer3-2-out	Y	Y	Y

Legend: Y: Can be set; N: Cannot be set

For each sending-side flow detection mode, see "Configuration Guide Vol. 2, 1.1.4 Sending-side flow detection mode".

Default behavior

The sending-side flow detection mode is set to layer3-1-out.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip access-group

ipv6 traffic-filter

mac access-group

flow rate-alarm

Enables the bandwidth non-compliance notification.

Syntax

To set or change information:

> flow rate-alarm [entry <entries>] [exceed-count <exceed count> <trial count>] [conform-count <conform count> <trial count>]

To delete information:

> no flow rate-alarm

Input mode

`(config)`

Parameters

entry <entries>

> Sets the number of QoS entries to be monitored per second. In a stack configuration, each member switch is monitored with the setting value of this parameter.
>
> 1. Default value when this parameter is omitted:
>
>   100
>
> 2. Range of values:
>
>   10 to 200

exceed-count <exceed count> <trial count>

> Configures the periodic monitoring conditions for QoS entries in bandwidth compliance status.
>
> <exceed count> is the number of bandwidth non-compliances. <trial count> is the number of times of monitoring.
>
> 1. Default value when this parameter is omitted:
>
>   <exceed count>: 1
>
>   <trial count>: 1
>
> 2. Range of values:
>
>   <exceed count>: 1 to 3600
>
>   <trial count>: 1 to 3600
>
>   <trial count> must be specified with a number equal to or greater than <exceed count>.

conform-count <conform count> <trial count>

> Configures the periodic monitoring conditions for QoS entries in bandwidth non-compliance status.
>
> <conform count>is the number of bandwidth compliances. <trial count> is the number of times of monitoring.
>
> 1. Default value when this parameter is omitted:
>
>   <conform count>: 300
>
>   <trial count>: 300
>
> 2. Range of values:

<conform count>: 1 to 3600

<trial count>: 1 to 3600

<trial count> must be specified with a number equal to or greater than <conform count>.

Default behavior

Bandwidth non-compliance notifications are not sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. After the setting values are changed, the monitoring status of the QoS entries is initialized, and monitoring is performed again.

2. If bandwidth non-compliance notifications are sent as operation messages and the bandwidth status changes frequently, other operation messages cannot be recorded. For this reason, it is recommended that you do not to set the conform-count parameter to a value less than the default value of 300.

Related commands

qos (ip qos-flow-list)

qos (ipv6 qos-flow-list)

qos (mac qos-flow-list)

25 Access Lists

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 25-1: 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

#: The protocol name ah or the protocol number 51 cannot be detected as a filter condition.

■ Protocol names (IPv6)

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

Table 25-2: 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

Protocol name	Applicable protocol number
sctp	132
tcp	6
tunnel	4
udp	17
vrrp	112

■ Port names (TCP)

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

Table 25-3: 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)

Port name	Applicable port name and number
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)
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 25-4: 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)

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

Table 25-5: 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)

Port name	Applicable port name and number
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

■ tos names

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

Table 25-6: 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 names

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

Table 25-7: 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 names

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

Table 25-8: 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
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 25-9: 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.

Ethernet type name	Ethernet value	Remarks
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 25-10: 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
slow-protocol	0180.C200.0002	0000.0000.0000

#:

This applies to IEEE 802.1AB/D6.0 frames only. Specify this with the value to target IEEE Std 802.1AB frames.

■ Message names (ICMP)

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

Table 25-11: 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

Message name	Message	Type	Code
host-isolated	Host isolated	3	8
host-precedence-unreach-able	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
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

Message name	Message	Type	Code
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 25-12: 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 advertise-ments	136	Not specified
nd-ns	Neighbor discovery neighbor solicita-tions	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
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

Message name	Message	Type	Code
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.

■ 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.

Specifications are counted separately for the receiving side and sending side. 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.

■ 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 25-13: 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 that can be created for use	Number of specifications that can be set for an interface

In this example, access list AAA is created and applied to inbound on Ethernet interface 1/0/1.
`interface gigabitethernet 1/0/1`
` ip access-group AAA in`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
	1 list	1 list

In this example, access list AAA is created and applied to inbound on Ethernet interfaces 1/0/1 and 1/0/2.
`interface gigabitethernet 1/0/1`
` ip access-group AAA in`
 	
`interface gigabitethernet 1/0/2`
` ip access-group AAA in`
 	
`ip access-list extended AAA`
` 10 permit tcp any any`
` 20 deny udp any any`
	1 list	2 lists

Sample code	Number of access lists that can be created for use	Number of specifications that can be set for an interface

In this example, access list AAA is created and applied to inbound and outbound on Ethernet interface 1/0/1.
 	
``
interface gigabitethernet 1/0/1
  ip access-group AAA in
  ip access-group AAA out
 	
ip access-list extended AAA
  10 permit tcp any any
  20 deny udp any any
``
	1 list	2 lists

In this example, access list AAA is created and applied to inbound on Ethernet interface 1/0/1.
In this example, access list BBB is created and applied to inbound on Ethernet interface 1/0/2.
 	
``
interface gigabitethernet 1/0/1
  ip access-group AAA in
 	
interface gigabitethernet 1/0/2
  ip access-group BBB in
 	
ip access-list extended AAA
  10 permit tcp any any
  20 deny udp any any
 	
ip access-list extended BBB
  10 permit udp any any
  20 deny tcp any any
``
	2 lists	2 lists

In this example, access list AAA is created and applied to inbound on Ethernet interface 1/0/1.
In this example, access list BBB is created and applied to outbound on Ethernet interface 1/0/1.
 	
``
interface gigabitethernet 1/0/1
  ip access-group AAA in
  ip access-group BBB out
 	
ip access-list extended AAA
  10 permit tcp any any
  20 deny udp any any
 	
ip access-list extended BBB
  10 permit udp any any
  20 deny tcp any any
``
	2 lists	2 lists

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

Sets an access list used as an IPv4 filter. There are two types of access lists that serve 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, ToS field value, port number, TCP flag, ICMP type, and ICMP code.

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

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device.

You can create a maximum of 2048 filter condition entries per IPv4 address filter or IPv4 packet filter.

A maximum of 1024 remark parameters can be specified for access lists and QoS flow lists per device.

For details about access lists, 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. [SL-L3A]

Syntax

To set or change information:

Configuring supplementary information

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

Configuring an IPv4 address filter

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

Configuring an IPv4 packet filter

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

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

filter-condition

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

  {deny | permit} {ip | <protocol>} {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

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

- When the upper layer protocol is UDP

  {deny | permit} udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  {deny | permit} icmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}
  {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{<icmp type>
  [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}]
  [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is IGMP

  {deny | permit} igmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}
  {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>]
  [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

Action specification SL-L3A

action policy-list <policy list no.>

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 (in decimal) 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 "■Arbitrary character string" in "Specifiable values for parameters".

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:

   None

{<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 IPv4 address.

   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 25-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard>| host <source ipv4> | any}

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>, or any.

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.

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

{eq <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 25-3: Port names that can be specified for TCP" and "Table 25-4: Port names that can be specified for UDP (IPv4)".

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

If 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> <destination ipv4 wildcard> | host <destination ipv4> | any}

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>, or any.

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.

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

{eq <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 25-3: Port names that can be specified for TCP" and "Table 25-4: Port names that can be specified for UDP (IPv4)".

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

   If 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos				-

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 25-6: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos				-

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 25-7: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

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 25-8: DSCP names that can be specified".

ack

Specifies the detection of packets whose ACK 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

fin

Specifies the detection of packets whose FIN 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

psh

Specifies the detection of packets whose PSH 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

rst

Specifies the detection of packets whose 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

syn

Specifies the detection of packets whose SYN 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

urg

Specifies the detection of packets whose URG 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

<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 25-11: 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

vlan <vlan id>

Specifies a VLAN ID.

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:

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 [SL-L3A]

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-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.

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. The protocol name ah and the protocol number 51 (in decimal) cannot be set in <protocol> as detection conditions for filtering.

7. 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 filter conditions: [SL-L3A]

- Source IPv4 address

  Multicast address and internal loopback address

- Destination IPv4 address

  Multicast address, restricted broadcast address, and internal loopback address

Related commands

ip access-group

ip access-list resequence

policy-list [SL-L3A]

deny (ip access-list extended)

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

Syntax

To set or change information:

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

  [<sequence>] deny {ip | <protocol>} {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

  [<sequence>] deny tcp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is UDP

  [<sequence>] deny udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  [<sequence>] deny icmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is IGMP

  [<sequence>] deny igmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

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 25-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}

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>, or any.

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.

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

{eq <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 25-3: Port names that can be specified for TCP" and "Table 25-4: Port names that can be specified for UDP (IPv4)".

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

If 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> <destination ipv4 wildcard> | host <destination ipv4> | any}

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>, or any.

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.

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

{eq <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 25-3: Port names that can be specified for TCP" and "Table 25-4: Port names that can be specified for UDP (IPv4)".

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

If 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos				-

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 25-6: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos				-

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 25-7: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

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 25-8: DSCP names that can be specified".

ack

Specifies the detection of packets whose ACK 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

fin

Specifies the detection of packets whose FIN 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

psh

Specifies the detection of packets whose PSH 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

rst

Specifies the detection of packets whose 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

syn

Specifies the detection of packets whose SYN 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

urg

Specifies the detection of packets whose URG 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

<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 25-11: 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

vlan <vlan id>

Specifies a VLAN ID.

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:

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.

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. The protocol name ah and the protocol number 51 (in decimal) cannot be set in <protocol> as detection conditions for filtering.

Related commands

access-list

ip access-group

ip access-list resequence

permit (ip access-list extended)

remark

deny (ip access-list standard)

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

Syntax

To set or change information:

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

To delete information:

    no <sequence>

Input mode

`(config-std-nacl)`

Parameters

<sequence>

    Specifies the sequence 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 IPv4 address.

    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

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:

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

  [<sequence>] deny {ipv6 | <protocol>} {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

  [<sequence>] deny tcp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [ack] [fin] [psh] [rst] [syn] [urg] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is UDP

  [<sequence>] deny udp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  [<sequence>] deny icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

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 25-2: Protocol names that can be specified (IPv6)".

{<source ipv6>/<length> | host <source ipv6> | any}

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>, 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.

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.

<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 <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 25-3: Port names that can be specified for TCP" and "Table 25-5: Port names that can be specified for UDP (IPv6)".

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

If 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> | any}

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>, host <destination ipv6>, or any.

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.

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.

<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 <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 25-3: Port names that can be specified for TCP" and "Table 25-5: Port names that can be specified for UDP (IPv6)".

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

If 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

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 25-8: DSCP names that can be specified".

ack

    Specifies the detection of packets whose ACK 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

fin

    Specifies the detection of packets whose FIN 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

psh

    Specifies the detection of packets whose PSH 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

rst

    Specifies the detection of packets whose 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

syn

    Specifies the detection of packets whose SYN 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

urg

    Specifies the detection of packets whose URG 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

<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 25-12: 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>

Specifies a VLAN ID.

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:

    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.

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

deny (mac access-list extended)

Specifies the conditions by which the MAC filter denies access.

Syntax

To set or change information:

> [<sequence>] deny {<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>] [user-priority <priority>]

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 function.

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 25-9: Ethernet type names that can be specified".

vlan <vlan id>

Specifies a VLAN ID.

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:

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.

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 25-10: 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

ip access-group

Applies an IPv4 access list to an Ethernet interface or a VLAN interface, and enables the IPv4 filter function. A maximum of 540 lists of ip access-group, ipv6 traffic-filter, and mac access-group can be set for interfaces per device.

For the number of specifications for the 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. [SL-L3A]

Syntax

To set information:

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

To delete information:

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

Input mode

`(config-if)`

Ethernet interface, VLAN interface

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 | in-mirror}

Specifies the inbound or outbound for the filter, or the inbound for policy-based mirroring.

in: Inbound for the filter (Specifies the receiving side)

out: Outbound for the filter (Specifies the sending side)

in-mirror: Inbound for policy-based mirroring (specifies the receiving side)

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

None

Impact on communication

When an access list with at least one entry is 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. You can set one IPv4 access list each for the inbound and outbound filters and the inbound policy-based mirroring on the same interface. 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. IPv4 packet filtering can be applied to an Ethernet interface where the "switchport mode stack" command is not set.

4. When IPv4 packet filtering is applied to an Ethernet interface, the flow detection mode can be set if a VLAN parameter exists as a flow detection condition and the VLAN ID is included in the Ethernet interface settings.

5. When IPv4 packet filtering is applied to a VLAN interface, the flow detection mode can be set if no VLAN parameters are included as a flow detection condition.

6. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if no tunneling ports have been set for the Ethernet interface for the device.

7. An access list can be set on the sending side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the device.

8. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if tag translation has not been set for the target interface.

9. You can set an access list on the sending side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.

10. If an access list with the policy-mirror-list parameter specified is used for a filter, the setting of the policy-mirror-list parameter is disabled.

11. If an access list with the policy-list parameter specified is used for policy-based mirroring, the policy-list parameter is disabled.

Related commands

access-list

ip access-list standard

ip access-list extended

ip access-list extended

Sets an access list used as an IPv4 filter. There are two types of access lists that serve 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, ToS field value, port number, TCP flag, ICMP type, and ICMP code.

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device.

You can create a maximum of 2048 filter condition entries per IPv4 address filter or IPv4 packet filter.

For details about access lists, 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. [SL-L3A]

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.
>
> > 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

Sets an access list used as an IPv4 filter. There are two types of access lists that serve 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.

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device.

You can create a maximum of 2048 filter condition entries per IPv4 address filter or IPv4 packet filter.

For details about access lists, 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.

      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

Sets an access list used 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, the traffic class field value, port number, TCP flag, ICMP type, and ICMP code.

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 filter condition entries can be created.

For details about access lists, see "■Number of access lists that can be created".

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.

   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 a VLAN interface, and enables the IPv6 filter function.

A maximum of 540 lists of ip access-group, ipv6 traffic-filter, and mac access-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

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

To delete information:

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

Input mode

`(config-if)`

Ethernet interface, VLAN interface

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 | in-mirror}

Specifies the inbound or outbound for the filter, or the inbound for policy-based mirroring.

in: Inbound for the filter (Specifies the receiving side)

out: Outbound for the filter (Specifies the sending side)

in-mirror: Inbound for policy-based mirroring (specifies the receiving side)

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

None

Impact on communication

When an access list with at least one entry is 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. You can set one IPv6 access list each for the inbound and outbound filters and the inbound policy-based mirroring on the same interface. If a filter has already been set, first remove it and then set it again.

2. If you specify a non-existent IPv6 filter, this will be ignored. The identifier of the IPv6 filter is registered.

3. IPv6 packet filtering can be applied to an Ethernet interface where the "switchport mode stack" command is not set.

4. If a VLAN parameters is included as a flow detection condition, the flow detection mode can be set if the VLAN ID is included in the Ethernet interface settings to be applied.

5. When IPv6 packet filtering is applied to a VLAN interface, the flow detection mode can be set if no VLAN parameters are included as a flow detection condition.

6. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if no tunneling ports have been set for the Ethernet interface for the device.

7. An access list can be set on the sending side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the device.

8. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if tag translation has not been set for the target interface.

9. You can set an access list on the sending side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.

10. If an access list with the policy-mirror-list parameter specified is used for a filter, the setting of the policy-mirror-list parameter is disabled.

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 filter function. A maximum of 540 lists of ip access-group, ipv6 traffic-filter, and mac access-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

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

To delete information:

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

Input mode

`(config-if)`

> Ethernet interface, VLAN interface

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 | in-mirror}

> Specifies the inbound or outbound for the filter, or the inbound for policy-based mirroring.
>
> in: Inbound for the filter (Specifies the receiving side)
>
> out: Outbound for the filter (Specifies the sending side)
>
> in-mirror: Inbound for policy-based mirroring (specifies the receiving side)
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   None

Default behavior

None

Impact on communication

When an access list with at least one entry is 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. You can set one MAC access list each for the inbound and outbound filters and the inbound policy-based mirroring on the same interface. 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. MAC filtering can be applied to an Ethernet interface where the "switchport mode stack" command is not set.

4. When a MAC filter is applied to an Ethernet interface, the flow detection mode can be set if a VLAN parameter exists as a flow detection condition and the VLAN ID is included in the Ethernet interface settings.

5. When a MAC filter is applied to a VLAN interface, the flow detection mode can be set if no VLAN parameters are included as a flow detection condition.

6. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if no tunneling ports have been set for the Ethernet interface for the device.

7. An access list can be set on the sending side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the device.

8. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if tag translation has not been set for the target interface.

9. You can set an access list on the sending side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.

10. If an access list with the policy-mirror-list parameter specified is used for a filter, the setting of the policy-mirror-list parameter is disabled.

Related commands

mac access-list extended

mac access-list extended

Sets an access list used as 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.

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 filter condition entries can be created.

For details about access lists, see "■Number of access lists that can be created".

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.

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

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

Syntax

To set or change information:

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

Input mode

`(config)`

Parameters

<access list name>

Specifies the 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 (ip access-list extended)

Specifies the conditions by which the IPv4 packet 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, ICMP, and IGMP

  {ip | <protocol>} {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

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

- When the upper layer protocol is UDP

  udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  icmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is IGMP

  igmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

Action specification

action policy-mirror-list <destination interface list name>

Action specification SL-L3A

action {policy-list <policy list no.> | policy-mirror-list <destination interface list name>}

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 25-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}

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>, or any.

   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.

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

{eq <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 25-3: Port names that can be specified for TCP" and "Table 25-4: Port names that can be specified for UDP (IPv4)".

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

If 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> <destination ipv4 wildcard> | host <destination ipv4> | any}

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>, or any.

   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.

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

{eq <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 25-3: Port names that can be specified for TCP" and "Table 25-4: Port names that can be specified for UDP (IPv4)".

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

   If 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos				-

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 25-6: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos			-	

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 25-7: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

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 25-8: DSCP names that can be specified".

ack

Specifies the detection of packets whose ACK 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

fin

Specifies the detection of packets whose FIN 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

psh

    Specifies the detection of packets whose PSH 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

rst

    Specifies the detection of packets whose 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

syn

    Specifies the detection of packets whose SYN 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

urg

    Specifies the detection of packets whose URG 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

<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 25-11: 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

vlan <vlan id>

Specifies a VLAN ID.

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:

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-list <policy list no.> [SL-L3A]

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-mirror-list <destination interface list name>

Specifies the name of the destination interface list for policy-based mirroring.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the name of the destination interface list that has already been set with the "destination-interface-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. The protocol name ah and the protocol number 51 (in decimal) cannot be set in <protocol> as detection conditions for filtering.

4. 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 filter conditions: [SL-L3A]

   • Source IPv4 address

   Multicast address and internal loopback address

   • Destination IPv4 address

   Multicast address, restricted broadcast address, and internal loopback address

Related commands

access-list

ip access-group

ip access-list resequence

deny (ip access-list extended)

remark

policy-list [SL-L3A]

destination-interface-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 IPv4 address.

   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} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

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

- When the upper layer protocol is UDP

  udp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length>| host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [{traffic-class <traffic class> | dscp <dscp>}] [{<icmp type> [<icmp code>] | <icmp message>}] [vlan <vlan id>] [user-priority <priority>]

Action specification

action policy-mirror-list <destination interface list name>

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 25-2: Protocol names that can be specified (IPv6)".

{<source ipv6>/<length> | host <source ipv6> | any}

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>, 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.

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.

<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 <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 25-3: Port names that can be specified for TCP" and "Table 25-5: Port names that can be specified for UDP (IPv6)".

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

If 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> | any}

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>, host <destination ipv6>, or any.

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.

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.

<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 <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 25-3: Port names that can be specified for TCP" and "Table 25-5: Port names that can be specified for UDP (IPv6)".

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

If 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

    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 25-8: DSCP names that can be specified".

ack

Specifies the detection of packets whose ACK 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

fin

Specifies the detection of packets whose FIN 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

psh

Specifies the detection of packets whose PSH 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

rst

Specifies the detection of packets whose 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

syn

Specifies the detection of packets whose SYN 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

urg

Specifies the detection of packets whose URG 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

<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 25-12: 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>

Specifies a VLAN ID.

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:

   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-mirror-list <destination interface list name>

Specifies the name of the destination interface list for policy-based mirroring.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the name of the destination interface list that has already been set with the "destination-interface-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.

Related commands

ipv6 traffic-filter

ipv6 access-list resequence

deny (ipv6 access-list)

remark

destination-interface-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>] [user-priority <priority>]

> Action specification

> action policy-mirror-list <destination interface list name>

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 function.

      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 25-9: Ethernet type names that can be specified".

vlan <vlan id>

      Specifies a VLAN ID.

      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:

      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-mirror-list <destination interface list name>

Specifies the name of the destination interface list for policy-based mirroring.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify the name of the destination interface list that has already been set with the "destination-interface-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 25-10: 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

deny (mac access-list extended)

remark

destination-interface-list

remark

Specifies supplementary information for the access list. Access lists are available for IPv4 address filtering, IPv4 packet filtering, IPv6 filtering, and MAC filtering. A maximum of 1024 information items can be specified for access lists and QoS flow lists per device.

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)
```

Parameters

<remark>

> Sets supplementary information for the target access list 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 "■Arbitrary 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

None

26 QoS

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 26-1: 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

#: The protocol name ah and the protocol number 51 cannot be detected as flow conditions.

■ Protocol names (IPv6)

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

Table 26-2: 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

Protocol name	Applicable protocol number
sctp	132
tcp	6
tunnel	4
udp	17
vrrp	112

■ Port names (TCP)

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

Table 26-3: 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)

Port name	Applicable port name and number
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)
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 26-4: 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)

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

Table 26-5: 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)

Port name	Applicable port name and number
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

■ tos names

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

Table 26-6: 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 names

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

Table 26-7: 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 names

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

Table 26-8: 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
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 26-9: Ethernet type names that can be specified

Ethernet type name	Ethernet value	Remarks
appletalk	0x809b	
arp	0x0806	
axp	0x88f3	Alaxala Protocol

Ethernet type name	Ethernet value	Remarks
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 26-10: 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
slow-protocol	0180.C200.0002	0000.0000.0000

#:

   This applies to IEEE 802.1AB/D6.0 frames only. Specify this with the value to target IEEE Std 802.1AB frames.

■ Message names (ICMP)

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

Table 26-11: 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

Message name	Message	Type	Code
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
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

Message name	Message	Type	Code
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 26-12: 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
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

Message name	Message	Type	Code
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 26-13: Range of values specifiable for bandwidth monitoring (10/100/1000BASE-T, 1000BASE-X)

Setting range		Increment
In Gbit/s[1]	1G	—
In Mbit/s[1]	1 M to 1000 M	1M
In kbit/s[1]	1000 to 1000000	100k[2]
	64 to 960	64k[3]

Legend: —: Not applicable

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...1000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192, 256...960).

Table 26-14: Range of values specifiable for bandwidth monitoring (10GBASE-R, 10GBASE-T)

Setting range		Increment
In Gbit/s[1]	1G to 10G	1G
In Mbit/s[1]	1M to 10000M	1M
In kbit/s[1]	1000 to 10000000	100k[2]
	64 to 960	64k[3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...10000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192, 256...960).

Table 26-15: Range of values specifiable for bandwidth monitoring (40GBASE-R)

Setting range		Increment
In Gbit/s[1]	1G to 40G	1G
In Mbit/s[1]	1M to 40000M	1M

Setting range		Increment
In kbit/s[#1]	1000 to 40000000	500k[#2]
	256 to 768	256k[#3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...40000000).

#3: When setting a value less than 1000 kbit/s, specify the value in units of 256 kbit/s (256, 512, and 768).

Table 26-16: Range of values specifiable for bandwidth monitoring (100GBASE-R)

Setting range		Increment
In Gbit/s[#1]	1G to 100G	1G
In Mbit/s[#1]	1M to 100000M	1M
In kbit/s[#1]	1000 to 100000000	500k[#2]
	256 to 768	256k[#3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...100000000).

#3: When setting a value less than 1000 kbit/s, specify the value in units of 256 kbit/s (256, 512, and 768).

■ 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.

■ 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.

■ 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 26-17: 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 that can be created for use	Number of specifications that can be set for an interface

In this example, QoS flow list AAA is created and applied to inbound on Ethernet interface 1/0/1.
 	
```interface gigabitethernet 1/0/1```
``` ip qos-flow-group AAA in```
 	
```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

Sample code	Number of QoS flow lists that can be created for use	Number of specifications that can be set for an interface
In this example, QoS flow list AAA is created and applied inbound on Ethernet interfaces 1/0/1 and 1/0/2. ``` interface gigabitethernet 1/0/1 ip qos-flow-group AAA in interface gigabitethernet 1/0/2 ip qos-flow-group AAA in 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 on Ethernet interface 1/0/1. In this example, QoS flow list BBB is created and applied to inbound on Ethernet interface 1/0/2. ``` interface gigabitethernet 1/0/1 ip qos-flow-group AAA in interface gigabitethernet 1/0/2 ip qos-flow-group BBB in 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

aggregate-policer

Sets the summarized bandwidth monitoring list. A maximum of 500 entries can be set.

Syntax

To set or change information:

aggregate-policer <aggregate name> in {<bps bandwidth policy> | <pps bandwidth policy>}

<bps bandwidth policy>

- When specifying maximum bandwidth monitoring in bit/s

  max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst {<kbyte> | <Mbyte>M}]

- When specifying minimum bandwidth monitoring in bit/s

  min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst {<kbyte> | <Mbyte>M}] [penalty-discard-class <class>] [penalty-dscp <dscp>]

When specifying maximum and minimum bandwidth monitoring in bit/s, the above specifications can be set in any order.

<pps bandwidth policy>

- When specifying maximum bandwidth monitoring in packet/s

  max-pps-rate <packet/s> [max-packet-burst <packet>]

- When specifying minimum bandwidth monitoring in packet/s

  min-pps-rate <packet/s> [min-packet-burst <packet>] [penalty-discard-class <class>] [penalty-dscp <dscp>]

When specifying maximum and minimum bandwidth monitoring in packet/s, the above specifications can be set in any order.

To delete information:

no aggregate-policer <aggregate name>

Input mode

`(config)`

Parameters

<aggregate name>

Specifies the summarized bandwidth monitoring 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".

<bps bandwidth policy> parameter

max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

Performs maximum bandwidth control in bit/s. Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value larger than min-rate.

max-rate-burst {<kbyte> | <Mbyte>M}

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:

   128

2. Range of values:

   <kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

   <Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

   If the monitoring bandwidth value for the maximum bandwidth control exceeds 10 G, a burst size of 32000, 64000, 32 M, or 64M can be specified.

   Specify a value larger than min-rate-burst.

min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

Performs minimum bandwidth monitoring in bit/s. 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-dscp to specify the penalty.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value smaller than max-rate.

min-rate-burst {<kbyte> | <Mbyte>M}

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:

   128

2. Range of values:

   <kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

   <Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

   If the monitoring bandwidth value for the minimum bandwidth monitoring exceeds 10G, a burst size of 32000, 64000, 32M, or 64M can be specified.

   Specify a value smaller than max-rate-burst.

<pps bandwidth policy> parameter

max-pps-rate <packet/s>

Performs maximum bandwidth control in packet/s. Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value larger than min-pps-rate.

max-packet-burst <packet>

Sets the burst size (the maximum number of packets that exceed the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value larger than min-packet-burst.

min-pps-rate <packet/s>

Performs minimum bandwidth monitoring in packet/s. 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-dscp to specify the penalty.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value smaller than max-pps-rate.

min-packet-burst <packet>

Sets the burst size (the minimum number of packets that fall below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value smaller than max-packet-burst.

<bps bandwidth policy> and <pps bandwidth policy>

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 or min-pps-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 3 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 or min-pps-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 26-8: DSCP names that can be specified".

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 summarized bandwidth monitoring list set as a QoS flow list cannot be deleted.

2. The penalty-dscp <dscp> parameter is not applied to MAC QoS flow lists.

3. If you set max-pps-rate to 2097152 or higher, the max-pps-rate value is rounded up to a multiple of 1024. If you set max-packet-burst to 2048 or higher, the max-packet-burst value is rounded up to a multiple of 512.

4. If you set min-pps-rate to 2097152 or higher, the min-pps-rate value is rounded up to a multiple of 1024. If you set min-packet-burst to 2048 or higher, the min-packet-burst value is rounded up to a multiple of 512.

5. For the burst size, set a value that satisfies the following formula for the monitoring bandwidth value of the corresponding maximum bandwidth control or minimum bandwidth monitoring. If the formula is not satisfied, bandwidth monitoring cannot be performed with the set monitoring bandwidth value.

[Formula for calculating the minimum burst size (bytes) for bandwidth monitoring in bit/s]

>Burst size (bytes) ≥ Monitoring bandwidth value (bit/s) / 8 (Conversion to bytes) / 8000

[Formula for calculating the minimum burst size (packets) for bandwidth monitoring in packet/s]

>Burst size (packets) ≥ Monitoring bandwidth value (packet/s) / 8000

Related commands

qos (ip qos-flow-list)

qos (ipv6 qos-flow-list)

qos (mac qos-flow-list)

ip qos-flow-group

Enables the QoS function by applying an IPv4 QoS flow list to an Ethernet interface or a VLAN interface. A maximum of 540 lists of ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

 ip qos-flow-group <qos flow list name> in

To delete information:

 no ip qos-flow-group <qos flow list name> in

Input mode

`(config-if)`

 Ethernet interface, VLAN interface

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

 Specifies Inbound.

 in: Inbound (Specifies the receiving side)

  1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

  2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can apply one IPv4 QoS flow list to the inbound side of an interface.

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. If another list has been set for an interface by using this command, no more lists can be set. Remove the existing list first, and then set another list.

4. An IPv4 QoS flow list can be applied to an Ethernet interface where the "switchport mode stack" command is not set.

5. When a list is to be applied to an Ethernet interface and a VLAN parameter exists as a flow detection condition, the list can be set if the VLAN ID is included in settings of the Ethernet interface.

6. If you apply a list to an Ethernet interface, you can apply the copy-user-priority parameter in the action specification if VLAN tunneling is configured.

7. If you apply a list to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection conditions and the copy-user-priority parameter is not set in the action specifications.

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. A maximum of 1024 QoS flow lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 flow detection and action specification entries can be created.

For details about the QoS flow lists, 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 the name of an IPv6 QoS flow list or MAC QoS flow list that has 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 function by applying an IPv6 QoS flow list to an Ethernet interface or a VLAN interface.

A maximum of 540 lists of ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

ipv6 qos-flow-group <qos flow list name> in

To delete information:

no ipv6 qos-flow-group <qos flow list name> in

Input mode

`(config-if)`

Ethernet interface, VLAN interface

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

Specifies Inbound.

in: Inbound (Specifies the receiving side)

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can apply one IPv6 QoS flow list to the inbound side of an interface.

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. If another list has been set for an interface by using this command, no more lists can be set. Remove the existing list first, and then set another list.

4. An IPv6 QoS flow list can be applied to an Ethernet interface where the "switchport mode stack" command is not set.

5. When a list is to be applied to an Ethernet interface and a VLAN parameter exists as a flow detection condition, the list can be set if the VLAN ID is included in settings of the Ethernet interface.

6. If you apply a list to an Ethernet interface, you can apply the copy-user-priority parameter in the action specification if VLAN tunneling is configured.

7. If you apply a list to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection conditions and the copy-user-priority parameter is not set in the action specifications.

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. A maximum of 1024 QoS flow lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 flow detection and action specification entries can be created.

For details about the QoS flow lists, 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 the name of an IPv4 QoS flow list or MAC QoS flow list that has 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

limit-queue-length

Sets the send queue length of a physical port for the Switch.

This command changes the maximum queue length of a physical port.

This command is used to set the basic conditions under which the hardware runs. You must restart the device after you change the settings.

If this command is not set or if the information set by using this command is deleted, a queue length of 2880 is used.

Syntax

To set or change information:

> limit-queue-length <queue length>

To delete information:

> no limit-queue-length

Input mode

`(config)`

Parameters

<queue length>

> Specifies the maximum queue length of a physical port.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   2880 or 24272

Default behavior

2880 is used as the send queue length for a port on a Switch.

Impact on communication

Communications that pass through the Switch stop while the Switch is restarting.

Restarting the VLAN program re-initializes all ports, and the ports that make up the VLAN temporarily become unable to send or receive data.

When the change is applied

If you have changed any values, save the configuration and restart the Switch or VLAN program. The new setting values take effect when restarting is performed.

Notes

1. Keep the following in mind:

   When 2880 has been set as the send queue length by using this command, the send queue length is as

follows:

Queues 1 to 12: 2880

When 24272 has been set as the send queue length by using this command, the send queue length is as follows:

Queue 1, queue 2: 24272; queue 3, queue 4: 2880; queues 5 to 12: 0

When you set a send queue length of 24272 by using this command, the queue length is allocated to only queue 1 and queue 4, resulting in the following scheduling behavior:

PQ: Queues 1 to 4 are processed based on the specified PQ.

4PQ+8RR: Queues 1 to 4 are processed based on RR.

4PQ+8WFQ: Queues 1 to 4 are processed based on WFQ.

4PQ+8ERR: Queues 1 to 4 are processed based on ERR.

4PQ+8WRR: Queues 1 to 4 are processed based on WRR.

Related commands

None

mac qos-flow-group

Enables the QoS function by applying a MAC QoS flow list to an Ethernet interface or a VLAN interface. A maximum of 540 lists of ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group can be set for interfaces per device.

For the number of specifications for the 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

To delete information:

no mac qos-flow-group <qos flow list name> in

Input mode

`(config-if)`

Ethernet interface, VLAN interface

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

Specifies Inbound.

in: Inbound (Specifies the receiving side)

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can apply one MAC QoS flow list to the inbound side of an interface.

2. If a non-existent MAC QoS flow list name is set, this will be ignored. The MAC QoS flow list name is registered.

3. If another list has been set for an interface by using this command, no more lists can be set. Remove the existing list first, and then set another list.

4. A MAC QoS flow list can be applied to an Ethernet interface where the "switchport mode stack" command is not set.

5. When a list is to be applied to an Ethernet interface and a VLAN parameter exists as a flow detection condition, the list can be set if the VLAN ID is included in settings of the Ethernet interface.

6. If you apply a list to an Ethernet interface, you can apply the copy-user-priority parameter in the action specification if VLAN tunneling is configured.

7. If you apply a list to a VLAN interface, you can set the list if no VLAN parameters are set in the flow detection conditions and the copy-user-priority parameter is not set in the action specifications.

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. A maximum of 1024 QoS flow lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 flow detection and action specification entries can be created.

For details about the QoS flow lists, 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 the name of an IPv4 QoS flow list or IPv6 QoS flow list that has 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

qos (ip qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv4 QoS flow list.

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, ICMP, and IGMP

{ip | <protocol> }{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

When the upper layer protocol is TCP

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

When the upper layer protocol is UDP

udp{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[{eq <source port> | range <source port start> <source port end>}]{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[{eq <destination port> | range <destination port start> <destination port end>}][{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

When the upper layer protocol is ICMP

icmp{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[{<icmp type> [<icmp code>] | <icmp message>}][{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

When the upper layer protocol is IGMP

igmp{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- **Action specification**

action [{[cos <cos>] [replace-user-priority <priority>] | copy-user-priority}] [discard-class <class>] [replace-dscp <dscp>] [{[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst {<kbyte> | <Mbyte>M}]] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst {<kbyte> | <Mbyte>M}] [penalty-discard-class <class>] [penalty-dscp <dscp>]] | [max-pps-rate <packet/s> [max-packet-burst <packet>]] [min-pps-rate <packet/s> [min-packet-burst <packet>] [penalty-discard-class <class>] [penalty-dscp <dscp>]] | aggregate-policer <aggregate name>}] [log] [trap]

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 26-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any }

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>, or any.

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.

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

{eq <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 26-3: Port names that can be specified for TCP" and "Table 26-4: 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 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> <destination ipv4 wildcard> | host <destination ipv4> | any }

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>, or any. 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.

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

{eq <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 26-3: Port names that can be specified for TCP" and "Table 26-4: 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 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos				-

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 26-6: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
precedence			tos				-

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 26-7: 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

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 26-8: DSCP names that can be specified".

ack

Specifies the detection of packets whose ACK 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

fin

Specifies the detection of packets whose FIN 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

psh

Specifies the detection of packets whose PSH 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

rst

Specifies the detection of packets whose 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

syn

Specifies the detection of packets whose SYN 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

urg

Specifies the detection of packets whose URG 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

<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 26-11: 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

vlan <vlan id>

Specifies a VLAN ID.

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:

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

cos <cos>

Specifies an index (CoS) indicating the priority on a device.

1. Default value when this parameter is omitted:

The default CoS values are set. For details about the default Cos values, see "Configuration Guide Vol. 2, 3.10.2 CoS values and queuing priority".

2. Range of values:

Specify 0 to 7 in decimal.

For details about specifying Cos values, see "Configuration Guide Vol. 2, 3.10.4 Note on using priority determination".

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 "Configuration Guide Vol. 2, 3.10.2 CoS values and queuing priority".
> >
> > 2. Range of values:
> >
> > Specify 1 to 3 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 26-8: 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.

copy-user-priority

> Enables the user priority inheritance function.
>
> For details about the user priority inheritance function, see "Configuration Guide Vol. 2, 3.7.2 User priority inheritance".
>
> > 1. Default value when this parameter is omitted:
> >
> > None. (The user priority inheritance function is not used.)
> >
> > 2. Range of values:
> >
> > None

max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

> Performs maximum bandwidth control in bit/s.
>
> Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.
>
> > 1. Default value when this parameter is omitted:
> >
> > None
> >
> > 2. Range of values:
> >
> > For details about specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value larger than min-rate.

max-rate-burst { <kbyte> | <Mbyte>M }

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:

128

2. Range of values:

<kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

<Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

If the monitoring bandwidth value for the maximum bandwidth control exceeds 10 G, a burst size of 32000, 64000, 32 M, or 64M can be specified.

Specify a value larger than min-rate-burst.

min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

Performs minimum bandwidth monitoring in bit/s.

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-dscp to specify the penalty.

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 specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value smaller than max-rate.

min-rate-burst { <kbyte> | <Mbyte>M }

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:

128

2. Range of values:

<kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

<Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

If the monitoring bandwidth value for the minimum bandwidth monitoring exceeds 10G, a burst size of 32000, 64000, 32M, or 64M can be specified.

Specify a value smaller than max-rate-burst.

max-pps-rate <packet/s>

Performs maximum bandwidth control in packet/s. Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value larger than min-pps-rate.

max-packet-burst <packet>

Sets the burst size (the maximum number of packets that exceed the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value larger than min-packet-burst.

min-pps-rate <packet/s>

Performs minimum bandwidth monitoring in packet/s. 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-dscp to specify the penalty.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value smaller than max-pps-rate.

min-packet-burst <packet>

Sets the burst size (the minimum number of packets that fall below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value smaller than max-packet-burst.

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 or min-pps-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 3 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 or min-pps-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 26-8: DSCP names that can be specified".

aggregate-policer <aggregate name>

Specifies the summarized bandwidth monitoring list name.

1. Default value when this parameter is omitted:

None

2. Range of values:

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

For details, see "Specifiable values for parameters".

log

Outputs an operation message when the bandwidth status is changed.

This parameter is enabled when one of the following bandwidth monitoring action parameters is set and the "flow rate-alarm" command is set.

- max-rate
- min-rate
- max-pps-rate
- min-pps-rate
- aggregate-policer

1. Default value when this parameter is omitted:

An operation message is not output.

2. Range of values:

None

trap

Sends an SNMP notification when the bandwidth status is changed.

This parameter is enabled when one of the following bandwidth monitoring action parameters is set and the "flow rate-alarm" command is set.

- max-rate
- min-rate
- max-pps-rate
- min-pps-rate
- aggregate-policer

1. Default value when this parameter is omitted:

SNMP notifications are not 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. 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. The protocol name ah and the protocol number 51 (in decimal) cannot be set in <protocol> as detection conditions for flow detection.

4. If a summarized bandwidth monitoring list name is specified for <aggregate name>, set the summarized bandwidth monitoring list name that was previously set with the "aggregate-policer" command.

5. If you set max-pps-rate to 2097152 or higher, the max-pps-rate value is rounded up to a multiple of 1024. If you set max-packet-burst to 2048 or higher, the max-packet-burst value is rounded up to a multiple of 512.

6. If you set min-pps-rate to 2097152 or higher, the min-pps-rate value is rounded up to a multiple of 1024. If you set min-packet-burst to 2048 or higher, the min-packet-burst value is rounded up to a multiple of 512.

7. For the burst size, set a value that satisfies the following formula for the monitoring bandwidth value of the corresponding maximum bandwidth control or minimum bandwidth monitoring. If the formula is not satisfied, bandwidth monitoring cannot be performed with the set monitoring bandwidth value.

   [Formula for calculating the minimum burst size (bytes) for bandwidth monitoring in bit/s]

   Burst size (bytes) ≥ Monitoring bandwidth value (bit/s) / 8 (Conversion to bytes) / 8000

   [Formula for calculating the minimum burst size (packets) for bandwidth monitoring in packet/s]

   Burst size (packets) ≥ Monitoring bandwidth value (packet/s) / 8000

Related commands

ip qos-flow-group

ip qos-flow-list resequence

remark

aggregate-policer

qos (ipv6 qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv6 QoS flow list.

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} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

  When the upper layer protocol is TCP

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

  When the upper layer protocol is UDP

  udp {<source ipv6>/<length> | host <source ipv6> | any} [{eq <source port> | range <source port start> <source port end>}] {<destination ipv6>/<length> | host <destination ipv6> | any} [{eq <destination port> | range <destination port start> <destination port end>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

  When the upper layer protocol is ICMP

  icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- Action specification
  action [{[cos <cos>] [replace-user-priority <priority>] | copy-user-priority}] [discard-class <class>] [replace-dscp <dscp>] [{[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst {<kbyte> | <Mbyte>M}]] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst {<kbyte> | <Mbyte>M}] [penalty-discard-class <class>] [penalty-dscp <dscp>]] | [max-pps-rate <packet/s> [max-packet-burst <packet>]] [min-pps-rate <packet/s> [min-packet-burst <packet>] [penalty-discard-class <class>] [penalty-dscp <dscp>]] | aggregate-policer <aggregate name>}] [log] [trap]

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 26-2: Protocol names that can be specified (IPv6)".

{<source ipv6>/<length> | host <source ipv6> | any}

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>, 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.

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.

<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 <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 26-3: Port names that can be specified for TCP" and "Table 26-5: Port names that can be specified for UDP (IPv6)".

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

If 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> | any}

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>, host <destination ipv6>, or any. 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.

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.

<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 <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 26-3: Port names that can be specified for TCP" and "Table 26-5: Port names that can be specified for UDP (IPv6)".

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

If 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.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

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 26-8: DSCP names that can be specified".

ack

Specifies the detection of packets whose ACK 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

fin

Specifies the detection of packets whose FIN 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

psh

Specifies the detection of packets whose PSH 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

rst

Specifies the detection of packets whose 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

syn

Specifies the detection of packets whose SYN 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

urg

    Specifies the detection of packets whose URG 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

<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 26-12: 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>

    Specifies a VLAN ID.

    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:

        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

cos <cos>

Specifies an index (CoS) indicating the priority on a device.

1. Default value when this parameter is omitted:

The default CoS values are set. For details about the default Cos values, see "Configuration Guide Vol. 2, 3.10.2 CoS values and queuing priority".

2. Range of values:

Specify 0 to 7 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 "Configuration Guide Vol. 2, 3.10.2 CoS values and queuing priority".

2. Range of values:

Specify 1 to 3 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 26-8: 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.

copy-user-priority

Enables the user priority inheritance function.

For details about the user priority inheritance function, see "Configuration Guide Vol. 2, 3.7.2 User priority inheritance".

1. Default value when this parameter is omitted:

   None. (The user priority inheritance function is not used.)

2. Range of values:

   None

max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

Performs maximum bandwidth control in bit/s.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   For specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value larger than min-rate.

max-rate-burst { <kbyte> | <Mbyte>M }

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:

   128

2. Range of values:

   <kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

   <Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

   If the monitoring bandwidth value for the maximum bandwidth control exceeds 10 G, a burst size of 32000, 64000, 32 M, or 64M can be specified.

   Specify a value larger than min-rate-burst.

min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

Performs minimum bandwidth monitoring in bit/s.

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-dscp to specify the penalty.

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 specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value smaller than max-rate.

min-rate-burst { <kbyte> | <Mbyte>M }

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:

128

2. Range of values:

<kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

<Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

If the monitoring bandwidth value for the minimum bandwidth monitoring exceeds 10G, a burst size of 32000, 64000, 32M, or 64M can be specified.

Specify a value smaller than max-rate-burst.

max-pps-rate <packet/s>

Performs maximum bandwidth control in packet/s. Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value larger than min-pps-rate.

max-packet-burst <packet>

Sets the burst size (the maximum number of packets that exceed the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value larger than min-packet-burst.

min-pps-rate <packet/s>

Performs minimum bandwidth monitoring in packet/s. 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-dscp to specify the penalty.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value smaller than max-pps-rate.

min-packet-burst <packet>

Sets the burst size (the minimum number of packets that fall below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value smaller than max-packet-burst.

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 or min-pps-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 3 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 or min-pps-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 26-8: DSCP names that can be specified".

aggregate-policer <aggregate name>

Specifies the summarized bandwidth monitoring list name.

1. Default value when this parameter is omitted:

None

2. Range of values:

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

For details, see "Specifiable values for parameters".

log

Outputs an operation message when the bandwidth status is changed.

This parameter is enabled when one of the following bandwidth monitoring action parameters is set and the "flow rate-alarm" command is set.

- max-rate
- min-rate
- max-pps-rate
- min-pps-rate
- aggregate-policer

1. Default value when this parameter is omitted:

An operation message is not output.

2. Range of values:

None

trap

Sends an SNMP notification when the bandwidth status is changed.

This parameter is enabled when one of the following bandwidth monitoring action parameters is set and the "flow rate-alarm" command is set.

- max-rate
- min-rate
- max-pps-rate
- min-pps-rate
- aggregate-policer

1. Default value when this parameter is omitted:

   SNMP notifications are not 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. 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 a summarized bandwidth monitoring list name is specified for <aggregate name>, set the summarized bandwidth monitoring list name that was previously set with the "aggregate-policer" command.

4. If you set max-pps-rate to 2097152 or higher, the max-pps-rate value is rounded up to a multiple of 1024. If you set max-packet-burst to 2048 or higher, the max-packet-burst value is rounded up to a multiple of 512.

5. If you set min-pps-rate to 2097152 or higher, the min-pps-rate value is rounded up to a multiple of 1024. If you set min-packet-burst to 2048 or higher, the min-packet-burst value is rounded up to a multiple of 512.

6. For the burst size, set a value that satisfies the following formula for the monitoring bandwidth value of the corresponding maximum bandwidth control or minimum bandwidth monitoring. If the formula is not satisfied, bandwidth monitoring cannot be performed with the set monitoring bandwidth value.

[Formula for calculating the minimum burst size (bytes) for bandwidth monitoring in bit/s]

   Burst size (bytes) ≥ Monitoring bandwidth value (bit/s) / 8 (Conversion to bytes) / 8000

[Formula for calculating the minimum burst size (packets) for bandwidth monitoring in packet/s]

   Burst size (packets) ≥ Monitoring bandwidth value (packet/s) / 8000

Related commands

ipv6 qos-flow-group

ipv6 qos-flow-list resequence

remark

aggregate-policer

qos (mac qos-flow-list)

Specifies flow detection conditions and action specifications in the MAC QoS flow list.

Syntax

To set or change information:

[<sequence>] qos {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>] [user-priority <priority>]

- Action specification

  action [{[cos <cos>] [replace-user-priority <priority>] | copy-user-priority}] [discard-class <class>] [{[max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [max-rate-burst {<kbyte> | <Mbyte>M}]] [min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G} [min-rate-burst {<kbyte> | <Mbyte>M}] [penalty-discard-class <class>]] | [max-pps-rate <packet/s> [max-packet-burst <packet>]] [min-pps-rate <packet/s> [min-packet-burst <packet>] [penalty-discard-class <class>]] | aggregate-policer <aggregate name> }] [log] [trap]

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 function.

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 26-9: Ethernet type names that can be specified".

vlan <vlan id>

Specifies a VLAN ID.

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:

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

cos <cos>

Specifies an index (CoS) indicating the priority on a device.

1. Default value when this parameter is omitted:

   The default CoS values are set. For details about the default Cos values, see "Configuration Guide Vol. 2, 3.10.2 CoS values and queuing priority".

2. Range of values:

   Specify 0 to 7 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 "Configuration Guide Vol. 2, 3.10.2 CoS values and queuing priority".

2. Range of values:

   Specify 1 to 3 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.

copy-user-priority

Enables the user priority inheritance function.

For details about the user priority inheritance function, see "Configuration Guide Vol. 2, 3.7.2 User priority inheritance".

1. Default value when this parameter is omitted:

   None. (The user priority inheritance function is not used.)

2. Range of values:

None

max-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

Performs maximum bandwidth control in bit/s.

Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

1. Default value when this parameter is omitted:

None

2. Range of values:

For specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value larger than min-rate.

max-rate-burst { <kbyte> | <Mbyte>M }

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:

128

2. Range of values:

<kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

<Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

If the monitoring bandwidth value for the maximum bandwidth control exceeds 10 G, a burst size of 32000, 64000, 32 M, or 64M can be specified.

Specify a value larger than min-rate-burst.

min-rate {<kbit/s> | <Mbit/s>M | <Gbit/s>G}

Performs minimum bandwidth monitoring in bit/s.

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 to specify the penalty.

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 specifiable monitoring bandwidth values, see "■Range of values specifiable for bandwidth monitoring". Specify a value smaller than max-rate.

min-rate-burst { <kbyte> | <Mbyte>M }

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:

128

2. Range of values:

<kbyte>: 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000

<Mbyte>M: 1M, 2M, 4M, 8M, 16M, 32M, 64M

If the monitoring bandwidth value for the minimum bandwidth monitoring exceeds 10G, a burst size of 32000, 64000, 32M, or 64M can be specified.

Specify a value smaller than max-rate-burst.

max-pps-rate <packet/s>

Performs maximum bandwidth control in packet/s. Bandwidth monitoring is performed for sent and received packets, and the packets that exceed the specified maximum bandwidth value are discarded.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value larger than min-pps-rate.

max-packet-burst <packet>

Sets the burst size (the maximum number of packets that exceed the maximum bandwidth and can be judged as a compliant packet) for maximum bandwidth control.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value larger than min-packet-burst.

min-pps-rate <packet/s>

Performs minimum bandwidth monitoring in packet/s. 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 to specify the penalty.

1. Default value when this parameter is omitted:

None

2. Range of values:

5 to 150000000

Specify a value smaller than max-pps-rate.

min-packet-burst <packet>

Sets the burst size (the minimum number of packets that fall below the minimum bandwidth and can be judged as a compliant packet) for minimum bandwidth monitoring.

1. Default value when this parameter is omitted:

512

2. Range of values:

1 to 2000000

Specify a value smaller than max-packet-burst.

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 or min-pps-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 3 in decimal.

aggregate-policer <aggregate name>

Specifies the summarized bandwidth monitoring list name.

1. Default value when this parameter is omitted:

None

2. Range of values:

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

For details, see "Specifiable values for parameters".

log

Outputs an operation message when the bandwidth status is changed.

This parameter is enabled when one of the following bandwidth monitoring action parameters is set and the "flow rate-alarm" command is set.

- max-rate
- min-rate
- max-pps-rate
- min-pps-rate
- aggregate-policer

1. Default value when this parameter is omitted:

An operation message is not output.

2. Range of values:

None

trap

Sends an SNMP notification when the bandwidth status is changed.

This parameter is enabled when one of the following bandwidth monitoring action parameters is set and the "flow rate-alarm" command is set.

- max-rate
- min-rate
- max-pps-rate
- min-pps-rate
- aggregate-policer

1. Default value when this parameter is omitted:

SNMP notifications are not 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. 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 26-10: 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 a summarized bandwidth monitoring list name is specified for <aggregate name>, set the summarized bandwidth monitoring list name that was previously set with the "aggregate-policer" command.

4. If you set max-pps-rate to 2097152 or higher, the max-pps-rate value is rounded up to a multiple of 1024. If you set max-packet-burst to 2048 or higher, the max-packet-burst value is rounded up to a multiple of 512.

5. If you set min-pps-rate to 2097152 or higher, the min-pps-rate value is rounded up to a multiple of 1024. If you set min-packet-burst to 2048 or higher, the min-packet-burst value is rounded up to a multiple of 512.

6. For the burst size, set a value that satisfies the following formula for the monitoring bandwidth value of the corresponding maximum bandwidth control or minimum bandwidth monitoring. If the formula is not satisfied, bandwidth monitoring cannot be performed with the set monitoring bandwidth value.

   [Formula for calculating the minimum burst size (bytes) for bandwidth monitoring in bit/s]

   Burst size (bytes) ≥ Monitoring bandwidth value (bit/s) / 8 (Conversion to bytes) / 8000

   [Formula for calculating the minimum burst size (packets) for bandwidth monitoring in packet/s]

   Burst size (packets) ≥ Monitoring bandwidth value (packet/s) / 8000

Related commands

mac qos-flow-group

mac qos-flow-list resequence

remark

aggregate-policer

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)`

    Ethernet interface

Parameters

<qos queue list name>

    Specifies the QoS queue list name.

    1. Default value when this parameter is omitted:

       This parameter cannot be omitted.

    2. Range of values:

       Specify a 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.

Impact on communication

If the scheduling mode is changed by specifying the QoS queue list name, the applicable 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 scheduling mode 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 an invalid QoS queue list name is specified by using the "qos-queue-group" command, PQ is used as the scheduling mode.

Related commands

qos-queue-list

qos-queue-list

Sets the scheduling mode in QoS queue list information. You can create no more than 100 lists per device.

Syntax

To set or change information:

> qos-queue-list <qos queue list name> { pq | 4pq+8rr | 4pq+8wfq [min-rate1 <minimum rate1>] [min-rate2 <minimum rate2>] [min-rate3 <minimum rate3>] [min-rate4 <minimum rate4>] [min-rate5 <minimum rate5>] [min-rate6 <minimum rate6>] [min-rate7 <minimum rate7>] [min-rate8 <minimum rate8>] | 4pq+8err <weight1> < weight2> < weight3> < weight4> < weight5> < weight6> < weight7> < weight8> | 4pq+8wrr <packet1> <packet2> <packet3> <packet4> <packet5> <packet6> <packet7> <packet8> }

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 | 4pq+8rr | 4pq+8wfq [min-rate1 <minimum rate1>] [min-rate2 <minimum rate2>] [min-rate3 <minimum rate3>] [min-rate4 <minimum rate4>] [min-rate5 <minimum rate5>] [min-rate6 <minimum rate6>] [min-rate7 <minimum rate7>] [min-rate8 <minimum rate8>] | 4pq+8err <weight1> < weight2> < weight3> < weight4> < weight5> < weight6> < weight7> < weight8> | 4pq+8wrr <packet1> <packet2> <packet3> <packet4> <packet5> <packet6> <packet7> <packet8> }

> Specifies the scheduling mode.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.

pq

> Sets priority queuing. The number of queues is fixed to 12 per physical port.
>
> If there are packets in multiple queues, packets with the highest priority queue number are always sent first (for example, packets in queue 12 are sent first, followed by packets in queue 11, and so on, until queue 1 is reached). Note that queues 12, 11, 10, and 9 are controlled so that each queue has an equal number of packets to be sent.
>
> When there are four queues, queues 4 and 3 are controlled so that each queue has an equal number of packets to be sent. If there is a packet in queue 4 or queue 3, the packet is sent with the highest priority. If there is no packet in queue 4 and queue 3, packets sent by queues 2 and 1 are evenly divided.

4pq+8rr

Round robin with top-priority queues. The number of queues is fixed to 12 per physical port.

For queues 12 to 9, priority queuing is used, and for queues 8 to 1, round robin is used. Queues 12 and 11 are controlled so that each queue has an equal number of packets to be sent. If queue 12 or 11 has packets, those packets are given priority and forwarded. Queues 10 and 9 are controlled so that each queue has an equal number of packets to be sent, and those packets are given priority next to queues 12 and 11 and forwarded. If there are no packets in queues 12 to 9, queues 8 to 1 are controlled so that each queue has an equal number of packets to be sent.

4pq+8wfq [min-rate1 <minimum rate1>] [min-rate2 <minimum rate2>] [min-rate3 <minimum rate3>] [min-rate4 <minimum rate4>] [min-rate5 <minimum rate5>] [min-rate6 <minimum rate6>] [min-rate7 <minimum rate7>] [min-rate8 <minimum rate8>]

Top-priority queues and weighted fair queuing. The number of queues is fixed to 12 per physical port.

For queues 12 to 9, priority queuing is used, and for queues 8 to 1, weighted fair queuing is used. Queues 12 and 11 are controlled so that each queue has an equal number of packets to be sent. If queue 12 or 11 has packets, those packets are given priority and forwarded. Queues 10 and 9 are controlled so that each queue has an equal number of packets to be sent, and those packets are given priority next to queues 12 and 11 and forwarded. If there are no packets in queues 12 or 9, packets of the minimum guaranteed bandwidth specified for each of the queues 8 to 1 as <minimum rate> are sent. Note that a number from 1 to 8 suffixed to <minimum rate> indicates a queue number.

1. Default value when this parameter is omitted:

   <minimum rate>: None. (A minimum guaranteed bandwidth is not set.)

2. Range of values:

   <minimum rate>: See the table below.

   You can specify k (default), M, or G for the unit of the value.

   { <minimum rate> | <minimum rate>M | <minimum rate>G }

   Specify <minimum rate> values so that their total value does not exceed the line bandwidth.

Table 26-18: Range of values for the minimum guaranteed bandwidth (10/100/1000BASE-T, 1000BASE-X)

Setting unit[#1]	Setting range	Increment
Gbit/s	1G	—
Mbit/s	1 M to 1000 M	1Mbit/s
kbit/s	1000 to 1000000	100 kbit/s[#2]
	64 to 960	64 kbit/s[#3]

Legend: —: Not applicable

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...1000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

Table 26-19: Range of values for the minimum guaranteed bandwidth (10GBASE-R, 10GBASE-T)

Setting unit[#1]	Setting range	Increment
Gbit/s	1G to 10G	1Gbit/s

Setting unit[1]	Setting range	Increment
Mbit/s	1M to 10000M	1Mbit/s
kbit/s	1000 to 10000000	100 kbit/s[2]
	64 to 960	64 kbit/s[3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...10000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

Table 26-20: Range of values for the minimum guaranteed bandwidth (40GBASE-R)

Setting unit[1]	Setting range	Increment
Gbit/s	1G to 40G	1Gbit/s
Mbit/s	1M to 40000M	1Mbit/s
kbit/s	1000 to 40000000	500 kbit/s[2]
	256 to 768	256 kbit/s[3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...40000000).

#3: When setting a value less than 1000 kbit/s, specify the value in units of 256 kbit/s (256, 512, and 768).

Table 26-21: Range of values for the minimum guaranteed bandwidth (100GBASE-R)

Setting unit[1]	Setting range	Increment
Gbit/s	1G to 100G	1Gbit/s
Mbit/s	1M to 100000M	1Mbit/s
kbit/s	1000 to 100000000	500 kbit/s[2]
	512	—

Legend: —: Not applicable

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...100000000).

4pq+8err <weight1> < weight2> < weight3> < weight4> < weight5> < weight6> < weight7> < weight8>

Top-priority queues and weighted (ratio based on the byte count) round robin. The number of queues is fixed to 12 per physical port.

For queues 12 to 9, priority queuing is used, and for queues 8 to 1, weighted fair queuing is used. Queues 12 and 11 are controlled so that each queue has an equal number of packets to be sent. If queue 12 or 11 has packets, those packets are given priority and forwarded. Queues 10 and 9 are controlled so that each queue has an equal number of packets to be sent, and those packets are given

priority next to queues 12 and 11 and forwarded. If there are no packets in queues 12 to 9, packets are sent according to the ratio based on the byte count set as <weight> of queues 8 to 1. A number from 1 to 8 suffixed to weight indicates the queue number.

1. Default value when this parameter is omitted:

   <weight>: This parameter cannot be omitted.

2. Range of values:

   <weight>: 1 to 127

4pq+8wrr <packet1> <packet2> <packet3> <packet4> <packet5> <packet6> <packet7> <packet8>

Top-priority queues and weighted (number of packets) round robin. The number of queues is fixed to 12 per physical port.

Queues 12 and 11 are controlled so that each queue has an equal number of packets to be sent. If queue 12 or 11 has packets, those packets are given priority and forwarded. Queues 10 and 9 are controlled so that each queue has an equal number of packets to be sent, and those packets are given priority next to queues 12 and 11 and forwarded. If there are no packets in queues 12 to 9, packets are sent according to the number of packets set for <packet> for queues 8 to 1. A number from 1 to 8 suffixed to packet indicates the queue number.

1. Default value when this parameter is omitted:

   <packet>: This parameter cannot be omitted.

2. Range of values:

   <packet>: 1 to 15

Default behavior

None

Impact on communication

If the scheduling mode 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 scheduling mode 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 WFQ is specified and the sum of the minimum guaranteed bandwidth exceeds the line bandwidth, unintended behavior may occur.

3. If WFQ is specified, there might be a maximum error of 10% between the set minimum guaranteed bandwidth and the actual value.

4. If WFQ is selected as the scheduling mode, <minimum rate> must be set for the queues that will be used.

Related commands

qos-queue-group

remark

Specifies supplementary information for a QoS flow list.

IPv4 QoS flow list, IPv6 QoS flow list, and MAC QoS flow list are available as QoS flow list. A maximum of 1024 information items can be specified for access lists and QoS flow lists per device.

Syntax

To set or change information:

> remark <remark>

To delete information:

> no remark

Input mode

```
(config-ip-qos)
(config-ipv6-qos)
(config-mac-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 "■Arbitrary 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

None

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 } [<kbyte>]

To delete information:

no traffic-shape rate

Input mode

`(config-if)`

Ethernet interface

Parameters

rate { <kbit/s> | <Mbit/s>M | <Gbit/s>G }

Sets port bandwidth control. Using this function limits the total-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.

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 26-22: Setting range for port bandwidth control (10/100/1000BASE-T, 1000BASE-X)

Setting unit[#1]	Setting range	Increment
Gbit/s	1G	—
Mbit/s	1 M to 1000 M	1Mbit/s
kbit/s	1000 to 1000000	100 kbit/s[#2]
	64 to 960	64 kbit/s[#3]

Legend: —: Not applicable

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...1000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

Table 26-23: Setting range for port bandwidth control (10GBASE-R, 10GBASE-T)

Setting unit[1]	Setting range	Increment
Gbit/s	1G to 10G	1Gbit/s
Mbit/s	1M to 10000M	1Mbit/s
kbit/s	1000 to 10000000	100 kbit/s[2]
	64 to 960	64 kbit/s[3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...10000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

Table 26-24: Setting range for port bandwidth control (40GBASE-R)

Setting unit[1]	Setting range	Increment
Gbit/s	1G to 40G	1Gbit/s
Mbit/s	1M to 40000M	1Mbit/s
kbit/s	1000 to 40000000	500 kbit/s[2]
	256 to 768	256 kbit/s[3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...40000000).

#3: When setting a value less than 1000 kbit/s, specify the value in units of 256 kbit/s (256, 512, and 768).

Table 26-25: Setting range for port bandwidth control (100GBASE-R)

Setting unit[1]	Setting range	Increment
Gbit/s	1G to 100G	1Gbit/s
Mbit/s	1M to 100000M	1Mbit/s
kbit/s	1000 to 100000000	500 kbit/s[2]
	512	—

Legend: —: Not applicable

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...100000000).

<kbyte>

Sets, in Kbytes, the burst size (tolerance to burst traffic) for port bandwidth control.

1. Default value when this parameter is omitted:

10/100/1000BASE-T, 1000BASE-X, 10GBASE-R, 10GBASE-T: 32

      40GBASE-R: 64

      100GBASE-R: 128

2. Range of values:

      10/100/1000BASE-T, 1000BASE-X, 10GBASE-R, 10GBASE-T: 4, 8, 16, 32

      40GBASE-R: 8, 16, 32, 64

      100GBASE-R: 16, 32, 64, 128

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. When the set bandwidth for port bandwidth control exceeds the line speed, the port bandwidth is not controlled.

2. Depending on the chip specifications, a burst communication of about 25 milliseconds occurs when the setting value is changed.

Related commands

None

27 Layer 2 Authentication

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 27-1: Configuration command and applicable Layer 2 authentication types

Command name	Applicable Layer 2 authentication types		
	IEEE 802.1X[#1]	Web authen-tication[#2]	MAC-based authentica-tion
authentication arp-relay	Y	Y	Y
authentication force-authorized enable	N	Y	Y
authentication force-authorized vlan	N	Y	Y
authentication ip access-group	Y	Y	Y
authentication max-user (global)	Y	Y	Y
authentication max-user (Ethernet interface)	Y	Y	Y
authentication radius-server dead-interval	N	Y	Y

Legend:

Y: The command can be set.

N: The command cannot be set. However, the command can be set if an applicable Layer 2 authentication coexists.

#1: For IEEE 802.1X, the command cannot be applied in single and multi modes of port-based authentication.

#2: For Web authentication, the command is applied in fixed and dynamic VLAN modes.

authentication arp-relay

Outputs ARP packets sent from unauthenticated terminals to other devices to a non-authenticating port.

Syntax

To set information:

authentication arp-relay

To delete information:

no authentication arp-relay

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

dot1x system-auth-control

mac-authentication system-auth-control

web-authentication system-auth-control

authentication force-authorized enable

When either of the following states exists for Web authentication and MAC-based authentication, this command forcibly changes the status of a terminal subject to authentication that requested authentication to the authenticated state:

- RADIUS authentication method is specified but there is no response from the designated RADIUS server

- Local authentication method is specified, but no authentication data exists on the device:
  - For Web authentication, this means that no users are registered in the internal Web authentication DB.
  - For MAC-based authentication, this means that no MAC addresses are registered in the internal MAC-based authentication DB.

Syntax

To set information:

authentication force-authorized enable

To delete information:

no authentication force-authorized 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. Be especially careful when using this function, as it can pose security problems.

2. If forced authentication is performed in Web authentication dynamic VLAN mode and MAC-based authentication dynamic VLAN mode, the native VLAN of the applicable port is assigned as the post-authentication VLAN. If you want to assign a specific VLAN as the post-authentication VLAN, do so by using the "authentication force-authorized vlan" command.

3. Web authentication and MAC-based authentication separately determine whether to perform forced authentication. Therefore, forced authentication might be performed by either authentication method.

Related commands

aaa authentication mac-authentication default group radius

aaa authentication web-authentication default group radius

mac-authentication port

mac-authentication system-auth-control

radius-server

web-authentication port

web-authentication system-auth-control

authentication force-authorized vlan

Assigns a post-authentication VLAN when forced authentication is performed on the applicable port in Web authentication dynamic VLAN mode and MAC-based authentication VLAN mode.

Syntax

To set or change information:

> authentication force-authorized vlan <vlan id>

To delete information:

> no authentication force-authorized vlan

Input mode

`(config-if)`

> Ethernet interface

Parameters

<vlan id>

> Sets a MAC VLAN as the post-authentication VLAN that is assigned when forced authentication is performed.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".
>
>   Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Default behavior

The native VLAN of the applicable port is assigned as the post-authentication VLAN.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

authentication force-authorized enable

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. Note that the Web authentication IP address is not treated as a destination IP address even when it is specified by using this command as a filtering condition.

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-if)`

> Ethernet interface

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

- If this command is not set, the following packets are not discarded before authentication:
  - Packets destined for the Web authentication IP address if such an IP address has been set
  - Packets destined for the http and https ports if URL redirection function has been set
- The IPv4 packet filter might be temporality disabled when any of the following operations is performed:
  - An existing filter condition is overwritten.
  - The "restart vlan" operation command is executed.
  - The "restart vlan mac-manager" operation command is executed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

dot1x system-auth-control

mac-authentication system-auth-control

web-authentication system-auth-control

authentication max-user (global)

Sets the maximum number of terminals that can be authenticated on a device for IEEE 802.1X authentication, Web authentication, and MAC-based authentication.

Syntax

To set or change information:

> authentication max-user <count>

To delete information:

> no authentication max-user

Input mode

`(config)`

Parameters

<count>

> Specifies the maximum number of terminals that can be authenticated on a device for IEEE 802.1X authentication, Web authentication, and MAC-based authentication.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 1024

Default behavior

The maximum number of terminals that can be authenticated on a device is 1024.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the maximum number of terminals that can be authenticated is changed to a value smaller than the number of terminals currently authenticated, the authenticated terminals can continue communication, but no more terminals can be authenticated.

2. The maximum number of terminals that can be authenticated on a device and a port can be set at the same time.

   - If the number of authenticated terminals reaches the maximum number allowed for port-based authentication terminals, no more terminals can be authenticated on the applicable port.
   - If the number of authenticated terminals reaches the maximum number for a device, no more terminals can be authenticated on that Switch.

Related commands

dot1x system-auth-control

mac-authentication system-auth-control

web-authentication system-auth-control

authentication max-user (Ethernet interface)

Sets the maximum number of terminals that can be authenticated on the applicable port for IEEE 802.1X authentication, Web authentication, and MAC-based authentication.

Syntax

To set or change information:

> authentication max-user <count>

To delete information:

> no authentication max-user

Input mode

`(config-if)`

> Ethernet interface

Parameters

<count>

> Specifies the maximum number of terminals that can be authenticated on the applicable port for IEEE 802.1X authentication, Web authentication, and MAC-based authentication.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 1024

Default behavior

The maximum number of authentication terminals that can be authenticated on the port is 1024.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the maximum number of terminals that can be authenticated is changed to a value smaller than the number of terminals currently authenticated, the authenticated terminals can continue communication, but no more terminals can be authenticated.

2. This setting is applied in IEEE 802.1X VLAN-based authentication (dynamic) mode and Web authentication legacy mode only when Web authentication dynamic VLAN mode or MAC-based authentication dynamic VLAN mode is set.

3. The maximum number of terminals that can be authenticated on a device and a port can be set at the same time.

   - If the number of authenticated terminals reaches the maximum number allowed for port-based authentication terminals, no more terminals can be authenticated on the applicable port.

- If the number of authenticated terminals reaches the maximum number for a device, no more terminals can be authenticated on that Switch.

Related commands

dot1x port-control

dot1x vlan

dot1x vlan dynamic

mac-authentication port

web-authentication port

authentication radius-server dead-interval

Specifies how long to wait before operation is resumed on the highest-priority RADIUS server after another server was used for Web authentication and MAC-based authentication and accounting due to a communication failure with the highest-priority RADIUS server.

The highest-priority RADIUS server resumes authentication and accounting after a specified time has elapsed. That interval starts from the time that another RADIUS server starts operation.

Syntax

To set or change information:

> authentication radius-server dead-interval <minutes>

To delete information:

> no authentication radius-server dead-interval

Input mode

`(config)`

Parameters

<minutes>

> Specifies, in minutes, the time that elapses before access to the highest-priority RADIUS server is made again after another RADIUS server starts operation.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   1 to 1440 (minutes)

Default behavior

The highest-priority RADIUS server starts again 10 minutes after another RADIUS server starts operation.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Because Web authentication and MAC-based authentication separately access the RADIUS server to check for communication failure, either authentication method might use the highest-priority RADIUS server while the other authentication method starts using another RADIUS server.

Related commands

None

28 IEEE 802.1X

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:

      None

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:

      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

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:

       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 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 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:
>
>   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 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 VLAN-based authentication (static), sets a specific port or channel group for which communication is permitted without authentication.

Syntax

To set information:

    dot1x force-authorized-port

To delete information:

    no dot1x force-authorized-port

Input mode

`(config-if)`

    Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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 logging enable

For IEEE 802.1X authentication, enables action 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

Action 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 action 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. Action tracking information is also logged.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The level of messages logged in the action 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)`

Ethernet interface, port channel interface

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)`

Ethernet interface, port channel interface

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 64

Default behavior

The maximum number of terminals that can be connected is 64.

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)`

Ethernet interface, port channel interface

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 authentication submode is set to single mode.

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)`

Ethernet interface, port channel interface

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 authentication submode is set to single mode.

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 function.

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)`

> Ethernet interface, port channel interface

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:
>
>   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 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. 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.

6. 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)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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 how terminal detection is performed when terminal authentication mode is specified as the authentication submode.

Syntax

To set or change information:

dot1x supplicant-detection {disable | full | shortcut | auto}

To delete information:

no dot1x supplicant-detection

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

{disable | full | shortcut | auto}

Configures how terminal detection is performed when terminal authentication mode is set as the authentication submode.

disable

If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. By receiving EAPOL-Start sent by the unauthenticated terminals, the unauthenticated terminals are detected and authentication is started.

For this reason, with this parameter specified, if you use the Supplicant software that cannot send EAPOL-Start spontaneously, unauthenticated terminals cannot be detected.

full

This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the authentication sequence is not skipped.

Since authenticated terminals periodically re-authenticate, a load proportional to the number of terminals is applied. When this parameter is specified, limit the number of terminals per authentication to 20 or less to avoid the impact of load.

shortcut

This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the load is reduced by omitting the authentication sequence and immediately sending EAP-Success.

However, some Supplicant software regards sending EAP-Success immediately as an authentication failure. As a result, when this parameter is specified, communication may be interrupted immediately after authentication, communication may be interrupted several minutes to several tens of minutes after authentication, or the load may increase due to repeated re-authentication.

If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. Instead, by receiving arbitrary frames sent by unauthenticated terminals, unauthenticated terminals are detected and authentication is started.

When this parameter is specified, terminals connected to a channel group cannot be detected by arbitrary receive frames. In this case, the only trigger for terminal detection is the reception of EAPOL-Start sent by the unauthenticated terminals.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

shortcut is used as the behavior 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 the EAPOL forwarding function 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 authentication submode is set to single mode. 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)`

> Ethernet interface, port channel interface

Parameters

<seconds>

> Specifies the period of time (in seconds) for maintaining communication-disabled state when the authentication submode is set to single mode.
>
> 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 on which the authentication submode is set to single mode.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x multiple-hosts

dot1x multiple-authentication

dot1x timeout quiet-period

Specifies the period of retention 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)`

> Ethernet interface, port channel interface

Parameters

<seconds>

> Specifies the period of retention 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 of retention time 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/Identity 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)`

> Ethernet interface, port channel interface

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 running 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 device 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. The "dot1x timeout reauth-period" 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)`

Ethernet interface, port channel interface

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 running 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)`

Ethernet interface, port channel interface

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 running 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)`

> Ethernet interface, port channel interface

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 running 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 device 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) function 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. The "dot1x vlan dynamic ignore-eapol-start" 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 "dot1x vlan dynamic ignore-eapol-start" 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 1024

Default behavior

The maximum number of terminals is 1024.

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 permit dynamic VLAN allocation according to VLAN information sent by 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 specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of 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. When VLANs are range-specified, an error will occur if not all of the VLANs can be set.

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 terminal is detected.

Syntax

To set or change information:

dot1x vlan dynamic supplicant-detection {disable | full | shortcut | auto}

To delete information:

no dot1x vlan dynamic supplicant-detection

Input mode

`(config)`

Parameters

{disable | full | shortcut | auto}

Specifies the behavior when a terminal is detected.

disable

If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. By receiving EAPOL-Start sent by the unauthenticated terminals, the unauthenticated terminals are detected and authentication is started.

For this reason, with this parameter specified, if you use the Supplicant software that cannot send EAPOL-Start spontaneously, unauthenticated terminals cannot be detected.

full

This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the authentication sequence is not skipped.

Since authenticated terminals periodically re-authenticate, a load proportional to the number of terminals is applied. When this parameter is specified, limit the number of terminals per authentication to 20 or less to avoid the impact of load.

shortcut

This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the load is reduced by omitting the authentication sequence and immediately sending EAP-Success.

However, some Supplicant software regards sending EAP-Success immediately as an authentication failure. As a result, when this parameter is specified, communication may be interrupted immediately after authentication, communication may be interrupted several minutes to several tens of minutes after authentication, or the load may increase due to repeated re-authentication.

auto

If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. Instead, by receiving arbitrary frames sent by unauthenticated terminals, unauthenticated terminals are detected and authentication is started.

When this parameter is specified, terminals connected to a channel group cannot be detected by ar-

bitrary receive frames. In this case, the only trigger for terminal detection is the reception of EAPOL-Start sent by the unauthenticated terminals.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

shortcut is used as the behavior 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.

4. If auto is specified in this command, communication using the pre-authentication native VLAN is restricted, and a pre-authentication filter is enabled.

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 retention 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 retention 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 of retention time 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/Identity 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 running 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 device 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 re-authentication" 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 running 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 running 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 running 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 device 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 specify <vlan id list> and the specifiable range of 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. When VLANs are range-specified, an error will occur if not all of the VLANs can be set.

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.

Related commands

vlan

dot1x system-auth-control

dot1x port-control

dot1x vlan dynamic radius-vlan

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 specify <vlan id list> and the specifiable range of 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 "dot1x vlan ignore-eapol-start" 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 specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of 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 terminal is detected.

Syntax

To set or change information:

> dot1x vlan <vlan id list> supplicant-detection {disable | full | shortcut | auto}

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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

{disable | full | shortcut | auto}

> Specifies the behavior when a terminal is detected.
>
> disable
>
>> If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. By receiving EAPOL-Start sent by the unauthenticated terminals, the unauthenticated terminals are detected and authentication is started.
>>
>> For this reason, with this parameter specified, if you use the Supplicant software that cannot send EAPOL-Start spontaneously, unauthenticated terminals cannot be detected.
>
> full
>
>> This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.
>>
>> The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the authentication sequence is not skipped.
>>
>> Since authenticated terminals periodically re-authenticate, a load proportional to the number of terminals is applied. When this parameter is specified, limit the number of terminals per authentication to 20 or less to avoid the impact of load.
>
> shortcut
>
>> This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.
>>
>> The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the load is reduced by omitting the authentica-

tion sequence and immediately sending EAP-Success.

However, some Supplicant software regards sending EAP-Success immediately as an authentication failure. As a result, when this parameter is specified, communication may be interrupted immediately after authentication, communication may be interrupted several minutes to several tens of minutes after authentication, or the load may increase due to repeated re-authentication.

auto

If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. Instead, by receiving arbitrary frames sent by unauthenticated terminals, unauthenticated terminals are detected and authentication is started.

When this parameter is specified, terminals connected to a channel group cannot be detected by arbitrary receive frames. In this case, the only trigger for terminal detection is the reception of EAPOL-Start sent by the unauthenticated terminals.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

shortcut is used as the behavior 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 retention 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 specify <vlan id list> and the specifiable range of 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 retention 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 of retention time 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/Identity 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 specify <vlan id list> and the specifiable range of 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 running 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 device 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 specify <vlan id list> and the specifiable range of 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 running 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 specify <vlan id list> and the specifiable range of 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 running 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 specify <vlan id list> and the specifiable range of 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 running 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 device 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

29 Web Authentication

Correspondence between configuration commands and running modes

The following table describes the Web authentication running modes in which Web authentication configuration commands can be set.

Table 29-1: Configuration commands and Web authentication running modes

Command name	Web authentication running 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 arp-relay	Y	Y	—
authentication force-authorized enable	Y	Y	—
authentication force-authorized vlan	—	Y	—
authentication ip access-group	Y	Y	—
authentication max-user (global)	Y	Y	—
authentication max-user (Ethernet interface)	Y	Y	—
authentication radius-server dead-interval	Y	Y	—
web-authentication auto-logout	—	Y	Y
web-authentication connection-pool level	Y	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	—	—

Command name	Web authentication running modes		
	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode
web-authentication logout polling re-try-interval	Y	—	—
web-authentication max-timer	Y	Y	Y
web-authentication max-user	—	Y	Y
web-authentication port	Y	Y	N
web-authentication redirect enable	Y	Y	—
web-authentication redirect-mode	Y	Y	—
web-authentication ssl connection-timeout	Y	Y	Y
web-authentication static-vlan max-user	Y	—	—
web-authentication system-auth-control	Y	Y	Y
web-authentication tcp-retransmission initial-timeout	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 function.

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 DB 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 connection-pool level

Sets the pool level of HTTP session connection.

Syntax

To set or change information:

web-authentication connection-pool level <level>

To delete information:

no web-authentication connection-pool level

Input mode

`(config)`

Parameters

Select the wait level of HTTP session connection.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 9

Default behavior

The wait level of the session connection is set to 5.

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. The lower the value of level is set, the shorter the connection waiting time. However, as the load increases, the number of forced disconnections increases, and the Web authentication screen may not be displayed.

2. The higher the value of level is set, the fewer forced disconnections will occur. However, under heavy load, the time to wait for the Web authentication screen may increase.

Related commands

web-authentication system-auth-control

web-authentication ip address

Set 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 device.

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.

Note that the IP address set by using this command is not treated as a destination IP address even when it is specified as a filtering condition by using the "authentication ip access-group" command.

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>

> Set 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 device, the IP address is not sent outside the device.

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 the "web-authentication ip address" 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 the "web-authentication ip address" command setting, 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://.....). (See the example below.)

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 "■Arbitrary 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 action 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

Action 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 function 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 device.

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

- To set the monitoring packet sending interval 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. One second is set by default.

Number of retransmissions

> The number of retransmissions set by using the "web-authentication logout polling count" command. Three retransmissions are 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 device.

   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 device.

   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

- To set the monitoring packet sending interval 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 device.

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 function 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 device.

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

- To set the monitoring packet sending interval 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 device.
>
> 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 one 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 function 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 device.

   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

- To set the monitoring packet sending interval 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 device. 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 users that can be authenticated in dynamic VLAN mode and legacy mode for Web authentication function.

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 1024

Default behavior

The maximum number of users that can be authenticated is 1024.

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)`
> Ethernet interface

Parameters

None

Default behavior

If this command has not been set, the Switch works 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. If a VLAN that sends and receives tagged frames is configured on a MAC VLAN port for which this command is specified, authentication is disabled on the VLAN.

4. 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 enable

Sets the URL redirect function for Web authentication.

If the "no web-authentication redirect enable" command is set, URL redirection is disabled.

Syntax

To set information:

    no web-authentication redirect enable

To delete information:

    web-authentication redirect enable

Input mode

`(config)`

Parameters

None

Default behavior

If this command is omitted, the URL redirect function is enabled.

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 is enabled when fixed VLAN mode or dynamic VLAN mode is set.
2. To set this command, you must also set the "web-authentication port" command.
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 port

web-authentication redirect-mode

web-authentication system-auth-control

web-authentication redirect-mode

Sets a protocol to display the Login page when the URL redirect function 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 function is enabled.

https

The Login page for https is displayed when the URL redirect function is enabled.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

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 is invalid if the "no web-authentication redirect enable" command is set.

Related commands

web-authentication port

web-authentication redirect enable

web-authentication system-auth-control

web-authentication ssl connection-timeout

Sets the timeout value for SSL session establishment.

Syntax

To set or change information:

web-authentication ssl connection-timeout <seconds>

To delete information:

no web-authentication ssl connection-timeout

Input mode

`(config)`

Parameters

<seconds>

Sets the timeout period in seconds to wait for an SSL session to be established.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 60

Default behavior

The timeout period for SSL session establishment is 60 seconds.

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 configuration applies to all HTTPS requests.
2. Under heavy load, SSL connections might be disconnected frequently.
3. The actual timeout period may be longer than the value specified in this configuration.

Related commands

web-authentication system-auth-control

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 1024

Default behavior

The maximum number of users that can be authenticated: 1024 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 Web authentication DB is saved in its current state.

2. 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 tcp-retransmission initial-timeout

Sets the initial timeout value for HTTP packet retransmission.

Syntax

To set or change information:

web-authentication tcp-retransmission initial-timeout <seconds>

To delete information:

no web-authentication tcp-retransmission initial-timeout

Input mode

`(config)`

Parameters

<seconds>

Sets the initial timeout period for HTTP packet retransmission.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 6

Default behavior

The initial timeout period for HTTP packet retransmission is one second.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This configuration applies to all HTTP/HTTPS requests. Under heavy load, the actual retransmission period may be longer than the value specified in this configuration.

Related commands

web-authentication system-auth-control

web-authentication vlan

Specifies the ID of a VLAN to permit VLAN switching in legacy mode for 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 specify <vlan id list> and the specifiable range of 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:
>>
>>   None

<port>

> Sets the communication port number for the 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, 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

30 MAC-based Authentication

Correspondence between configuration commands and running modes

The following table describes MAC-based authentication running modes in which MAC-based authentication configuration commands can be set.

Table 30-1: Configuration commands and MAC-based authentication running modes

Command name	MAC-based authentication running 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 arp-relay	Y	Y
authentication force-authorized enable	Y	Y
authentication force-authorized vlan	—	Y
authentication ip access-group	Y	Y
authentication max-user (global)	Y	Y
authentication max-user (Ethernet interface)	Y	Y
authentication radius-server dead-interval	Y	Y
mac-authentication auth-interval-timer	Y	Y
mac-authentication auto-logout	Y	Y
mac-authentication dot1q-vlan force-authorized	—	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 function.

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 DB 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 device. 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 authentication 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. By default or when this command is deleted, the Switch can be configured to cancel authentication when a not-accessed state is detected for a MAC address being authenticated by MAC-based authentication. In this case, authentication is canceled if the terminal with that MAC address remains unused for about 10 minutes after the aging time for the MAC address table expires and a not-accessed state is detected.

Related commands

max-authentication system-auth-control

mac-address-table aging-time

mac-authentication dot1q-vlan force-authorized

Permits terminals that send and receive tagged frames on a MAC VLAN port to communicate without being authenticated.

Syntax

To set information:

mac-authentication dot1q-vlan force-authorized

To delete information:

no mac-authentication dot1q-vlan force-authorized

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

Terminals that send and receive tagged frames on the target port are authenticated in fixed VLAN mode.

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 terminals that send tagged frames destined for the VLAN ID specified with the dot1q vlan parameter of the "switchport mac" command on ports configured by the "switchport mode" command with the mac-vlan parameter.

2. Terminals permitted to communicate without authentication are treated as terminals permitted by MAC-based authentication. Therefore, consider the following:

   • Maximum number of authenticated terminals per device and per port
   • Displaying information by using an operation command

Related commands

mac-authentication port

mac-authentication system-auth-control

switchport mac dot1q vlan

switchport mode mac-vlan

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 1024

Default behavior

The maximum number of MAC addresses that can be authenticated:

> 1024

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 action 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

Action 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 canceled 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 device. 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 "■Arbitrary 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.

However, fixed VLAN mode is set for a VLAN that sends and receives tagged frames and is configured on the port on which a MAC VLAN is set.

Syntax

To set information:

mac-authentication port

To delete information:

no mac-authentication port

Input mode

`(config-if)`

Ethernet interface

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 vlan <vlan id>] | <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 vlan <vlan id>] | <host name>}

Input mode

`(config)`

Parameters

{<ipv4 address> | <ipv6 address> [interface vlan <vlan id>] | <host name>}

> <ipv4 address>
>
>> Specifies the IPv4 address of the RADIUS server in dot notation.
>
> <ipv6 address> [interface vlan <vlan id>]
>
>> Specifies the IPv6 address of the RADIUS server in colon notation.
>>
>> Specify the interface parameter only when a link-local address is specified.
>>
>> - interface vlan <vlan id>
>>
>>   For <vlan id>, specify the VLAN ID set by the "interface vlan" command.
>
> <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 "■Arbitrary 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 priority over the information set by using the "radius-server host" command.

2. A maximum of four RADIUS servers per device 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 1024

Default behavior

The maximum number of MAC addresses that can be authenticated: 1024

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

None

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 function, 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 "■Arbitrary 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

31 **DHCP snooping**

ip arp inspection limit rate

Sets the maximum ARP packet reception rate (the number of ARP packets that can be received per second) per device 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 (packet/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 that the Switch will work properly up to the specified number of received packets.

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)`

> Ethernet interface, port channel interface

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 <item> [<item> [<item>]]

To delete information:

> no ip arp inspection validate

Input mode

`(config)`

Parameters

<item> [<item> [<item>]]

> Specifies an inspection item in <item>.
>
> For <item>, select one or two of the following: src-mac, dst-mac, and ip, or set them all. You cannot set the same <item> more than once.
>
> 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.
>
> 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.
>
> ip
>
> > This inspection item checks if the destination 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:
>
>   At least one of them must be set. Omitted items are not inspected.
>
> 2. Range of values:
>
>   src-mac, dst-mac, ip

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 range of 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 range of 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 range of 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

None

Related commands

None

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.

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

   • 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 device 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
   - 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 device 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

Permits 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 device. DHCP 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 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>

> Sets 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 (packet/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 that the Switch will work properly up to the specified number of received packets.

Related commands

ip dhcp snooping

ip dhcp snooping logging enable

Enables the output of DHCP snooping action 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

Action 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 action 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. Action tracking information is also logged.

  1. Default value when this parameter is omitted:

     This parameter cannot be omitted.

  2. Range of values:

     None

Default behavior

The level of messages to be logged in an action 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)`

> Ethernet interface, port channel interface

Parameters

None

Default behavior

The applicable interface serves 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>

Specifies 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 range of 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 range of 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 range of 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 a 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>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

- Ethernet interface
- Port channel interface

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 function 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)`

    Ethernet interface, port channel interface

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:

        None

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.

3. This command cannot be set if none of the following parameter values is specified in the "flow detection mode" command.

- layer3-dhcp-1
- layer3-suppress-dhcp-1
- dhcp-filter (specified for custom)

Related commands

flow detection mode

ip dhcp snooping

ip dhcp snooping trust

ip dhcp snooping vlan

ip source binding

32 GSRP

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 works as follows:

In master status:

Maintains master status.

In backup status:

Changes to backup status (neighbor unknown) because the partner device 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 five 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 one 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 adjacent 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 a 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 GSRP VLAN group-only control function, which is set by the "gsrp limit-control" command. If GSRP VLAN group-only control function is not set, the ports will be blocked.

Related commands

None

gsrp-vlan

Specify 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)`

Ethernet interface, port channel interface

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)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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 GSRP VLAN group-only control function.

If GSRP VLAN group-only control function 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 of 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)

Ethernet interface, port channel interface

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 function 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)`

    Ethernet interface, port channel interface

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

    Configure 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 function 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 function, also set this command for the partner device.
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 device.

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 running 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 ("set gsrp master" operation 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 a failure state, the Switch starts running as the master. To make a GSRP switch automatically run as the master when it is independently started by using the function for switchover to master status by an independently started GSRP switch, set the forced-shift-time parameter.

>> 1. Default value when this parameter is omitted:

>> This parameter cannot be omitted.

>> 2. Range of values:

>> For <seconds>, specify the time (in seconds) to wait until the GSRP switch automatically starts running as the master when it is independently started. You can specify the time in the range from 0 to 3,600 seconds.

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 running mode in which a GSRP switch changes from backup (neighbor unknown) status to master status, the Switch starts running as the master when all ports specified for a direct link are in a failure state.

   However, after the events 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 device
   - 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

2. A GSRP switch automatically changes from backup status to master status (by using the function 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 events is performed:

   - Execution of the "restart vlan" operation command
   - Executing the "restart gsrp" operation command
   - Applying the setting to the running configuration by using the "copy" operation command

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 ports, 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 (seconds) 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

Set 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 three 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 priority of the conditions for selecting the master and backup GSRP switches (number of active ports, priority, and device 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 priority 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 device are selected in that order.

priority-ports-mac

The priority, the number of active ports, and the MAC address of the device are selected in that order.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The number of active ports, the priority, and the MAC address of the device 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

virtual-mac-learning-interval

Sets the sending interval for frames for virtual MAC address learning to be sent when using Layer 3 redundancy switching function.

Syntax

To set or change information:

> virtual-mac-learning-interval <seconds>

To delete information:

> no virtual-mac-learning-interval

Input mode

`(config-gsrp)`

Parameters

<seconds>

> Specifies the sending interval (in seconds) for frames for virtual MAC address learning.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   4 to 120

Default behavior

The sending interval for frames for virtual MAC address learning is 120 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the sending interval is set to a short interval by using this command, there might be VLAN ports that cannot send frames depending on the number of VLAN ports where the frames for virtual MAC address learning is sent. In such cases, set the sending interval to a longer interval.

Related commands

layer3-redundancy

vlan-group disable

Disables the GSRP function 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 64

Default behavior

The GSRP function 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 64

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 64

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 specify \<vlan id list> and the specifiable range of 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 specify \<vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The same VLAN cannot be designated in more than one VLAN group.

Related commands

vlan

33 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 failure has occurred or whether the interface has recovered from a failure. 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 six 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 failure has occurred or whether the interface has recovered from a failure.

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 failure has occurred or whether the interface has recovered from a failure. 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 failure has occurred or whether the interface has recovered from a failure 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 related to a fault monitoring interface.

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 related to an interface. 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 two 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 related to a fault monitoring interface.

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 monitor only the interface status or to perform VRRP polling.

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>

> Specifies 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 fault monitoring interface.
>
> ip routing
>
> > Performs VRRP polling.
> >
> > > 1. Default value when this parameter is omitted:
> > >
> > > This parameter cannot be omitted.
> > >
> > > 2. Range of values:
> > >
> > > None

\<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\>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".
> >
> > - Ethernet interface
> >
> > - Port channel interface
> >
> > When using 100BASE-TX/1000BASE-T/10GBASE-T ports for 100BASE-TX/1000BASE-T, an Ethernet interface is specified with the "interface tengigabitethernet" command, but this parameter must be specified as gigabitethernet.
> >
> > When using SFP+/SFP shared ports for 10BASE-T/100BASE-TX/1000BASE-T or 1000BASE-X, an Ethernet interface is specified with the "interface tengigabitethernet" command, but this parameter must be specified as gigabitethernet.
> >
> > When using QSFP28/QSFP+ shared ports for 40GBASE-R, an Ethernet interface is specified with the "interface hundredgigabitethernet" command, but this parameter must be specified as fortygigabitethernet.

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 maximum of 255 fault monitoring interfaces can be set per device.

2. An IP address must be assigned to the VLAN interface that will be monitored for failures.

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, fault monitoring interface is performed.

Related commands

ip address

track ip route

vrrp ip

vrrp track

track ip route

Sets the destination address for VRRP polling when VRRP polling is performed with a fault monitoring interface.

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 or 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. 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 related to a fault monitoring interface.

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 two 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 related to a fault monitoring interface.

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 status 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)

VLAN interface

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)`

VLAN interface

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 "■Arbitrary 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 has been set for an IPv6 virtual router.

2. This setting is disabled if the "vrrp follow" command is set.

Related commands

None

vrrp follow

Specify the primary virtual router and set the virtual router as the follower virtual router. The track function, priority setting, PREEMPT mode setting, VRRP running mode setting, and advertisement packet sending interval setting set for the follower virtual router are disabled, and the virtual router follows the behavior 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)`

> VLAN interface

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 "■Arbitrary 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 IPv4 address owner.

2. This command cannot be set if the virtual router has been specified as a primary virtual router by another virtual router. Also, the virtual router name or follower virtual router name cannot be specified as the name of the virtual router itself.

3. This command cannot be set if the "vrrp ipv6" command has been set for the specified primary virtual router.

Related commands

vrrp name

vrrp ietf-ipv6-spec-07-mode

Sets an IPv6 virtual router to work 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)`

VLAN interface

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 works according to draft-ietf-vrrp-ipv6-spec-02.

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 devices that establish VRRP, the status 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 devices that establish VRRP, multiple master routers exist temporarily. After the settings for the devices are completed (as the same setting), only one master router is selected automatically.

3. When you enter this setting, if the setting value set by the "vrrp timers advertise" command exceeds 40, the sending interval of advertisement packets will be one second (default).

Related commands

ipv6 address

vrrp ipv6

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)`

VLAN interface

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 device is 255.

2. After an IP address is assigned to a virtual router by this command, the virtual router starts running.

3. A virtual router for which the "vrrp follow" command is 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)`

VLAN interface

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 device is 255.

2. After an IPv6 address is assigned to a virtual router by this command, the virtual router starts running.

3. This command cannot be set for a virtual router for which the "vrrp follow" command is set.

Related commands

ipv6 address

vrrp name

Sets a name for the virtual router.

Syntax

To set information:

vrrp <vrid> name <string>

To delete information:

no vrrp <vrid> name

Input mode

`(config-if)`

VLAN interface

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>

Sets a name for the virtual router.

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 "■Arbitrary 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 using the tracking function. If the priority of the virtual router is 0, the IP interface for which the virtual router is set will not go 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)`

> VLAN interface

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 priority 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 disabled if the "vrrp follow" command is set.

Related commands

None

vrrp preempt delay

Sets a period of time for suppressing automatic switchbacks. If automatic switchbacks are enabled, switch-back 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)`

VLAN interface

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 automatic switchback suppression time 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 disabled if the "vrrp follow" command is 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)`

    VLAN interface

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 works 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 disabled if the "vrrp follow" command is 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>

To delete information:

no vrrp <vrid> timers advertise

Input mode

(config-if)

VLAN interface

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

Default behavior

The sending interval of advertisement packets is set to one second.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the "vrrp ietf-ipv6-spec-07-mode" command is set, specification of a value larger than 40 is ignored, and one second (default) is used.

2. This setting is disabled if the "vrrp follow" command is set.

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)

VLAN interface

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 disabled if the "vrrp follow" command is set.

Related commands

vrrp preempt

vrrp track

Allocates a fault monitoring interface (track) to 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)`
> VLAN interface

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 to be set to the virtual router when a fault monitoring interface goes down.

> priority <priority>

>> Specifies the priority to be set to the virtual router when a fault monitoring interface goes down, 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 fault monitoring interface for which the priority parameter is specified can be set per virtual router.

> decrement <priority>

>> Specify a value to be subtracted from the current priority value of the virtual router when a fault monitoring interface goes down, in the range from 1 to 255. Multiple fault monitoring interfaces 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 "vrrp track priority" command can allocate one fault monitoring interface per virtual router.

2. To use the "vrrp track decrement" command to allocate additional fault monitoring interfaces to a virtual router to which a fault monitoring interface has been allocated by the "vrrp track priority" command, delete the allocated fault monitoring interface.

3. To use the "vrrp track priority" command to allocate a fault monitoring interface to a virtual router to which fault monitoring interfaces have been allocated by the "vrrp track decrement" command, delete all fault monitoring interfaces.

4. This setting is disabled if the "vrrp follow" command is set.

Related commands

track interface

34 Uplink Redundancy

switchport backup flush-request transmit

Enables the sending of flush control frames to upstream switches at switchover or switchback to request that the upstream switches clear their MAC address tables. This command takes effect when it is set for the primary port.

Syntax

To set or change information:

> switchport backup flush-request transmit [vlan <vlan id>]

To delete information:

> no switchport backup flush-request transmit

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

vlan <vlan id>

> Specifies the VLAN ID of the VLAN to which flush control frames are to be sent.
>
> 1. Default value when this parameter is omitted:
>
>   If the interface is to be set for an access port, flush control frames are sent to an access VLAN. For a trunk port, MAC VLAN port, and protocol VLAN port, flush control frames are sent to a native VLAN.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".

Default behavior

Flush control frames are not sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set this command for the primary port. This function is not enabled when the command is set for the secondary port.

2. This function cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface for which this function is set cannot be set for a channel group. Set this function for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

None

switchport backup interface

Sets a primary port and a secondary port for uplink redundancy and the automatic switchback time.

Syntax

To set or change information:

switchport backup interface <interface type> <interface number> [preemption-delay <seconds>]

To delete information:

no switchport backup interface

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

<interface type> <interface number>

Specifies a secondary port for uplink redundancy. The interface on which this command is set will be the primary port.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

   • Ethernet interface
   • Port channel interface

preemption-delay <seconds>

Sets the automatic switchback wait time. If you specify 0 seconds, a switchback is immediately performed.

1. Default value when this parameter is omitted:

   An automatic switchback is not performed.

2. Range of values:

   0 to 300 (seconds)

Default behavior

Uplink redundancy is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If this function is disabled, the ports in the standby state are also enabled for communication. This might cause loops. Shut down the primary port or the secondary port to prevent loops, and then disable this function.

2. You cannot specify an Ethernet interface that is part of a channel group as the primary port or the secondary port. Also, an Ethernet interface set as the primary port or secondary port cannot be set for a channel group. Set the primary port and secondary port for the port channel interface to which the applicable Ethernet interface belongs.

3. In a stack configuration, a primary port and secondary port of uplink redundancy cannot be set for one member switch.

4. In a stack configuration, this command cannot be set for a port channel interface of a channel group in which ports of multiple member switches are registered.

Related commands

None

switchport backup mac-address-table update exclude-vlan

Sets the VLAN to be excluded when sending MAC address update frames.

Syntax

To set information:

> switchport backup mac-address-table update exclude-vlan <vlan id list>

To change information:

> switchport backup mac-address-table update exclude-vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

To delete information:

> no switchport backup mac-address-table update exclude-vlan

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

<vlan id list>

> Sets the VLAN to be excluded when sending MAC address update frames. 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 specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of 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 specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

MAC address update frames are sent to all VLANs included on the primary port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, a change in the <vlan id list> value is applied the next time a switch or switchback is performed.

Notes

1. Setting the "switchport-backup mac-address-table update transmit" command enables this command.

2. Set this command for the primary port.

Related commands

None

switchport backup mac-address-table update transmit

Enables the sending of MAC address update frames and sets the number of times the frames are sent to request that the upstream switches update their MAC address tables.

Syntax

To set or change information:

> switchport backup mac-address-table update transmit [count <count>]

To delete information:

> no switchport backup mac-address-table update transmit

Input mode

`(config-if)`

> Ethernet interface, port channel interface

Parameters

count <count>

> Specifies the number of times MAC address update frames are sent.
>
> 1. Default value when this parameter is omitted:
>
>   1
>
> 2. Range of values:
>
>   1 to 3

Default behavior

MAC address update frames are not sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, the value set for the count parameter is applied the next time a switch or switchback is performed.

Notes

1. Set this command for the primary port.

Related commands

None

switchport backup reset-flush-port

Specifies a port on which port resetting is performed.

Syntax

To set information:

switchport backup reset-flush-port

To delete information:

no switchport backup reset-flush-port

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set this command for the primary port. This function is not enabled when the command is set for the secondary port.

2. This function cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface for which this function is set cannot be set for a channel group. Set this function for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

None

switchport backup reset-flush-time

Set the port-down time to be applied when port resetting is used.

Syntax

To set or change information:

switchport backup reset-flush-time <seconds>

To delete information:

no switchport backup reset-flush-time

Input mode

`(config-if)`

Ethernet interface, port channel interface

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 three seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The setting of this command is enabled when the "switchport backup reset-flush-port" command has been set.

Related commands

switchport backup reset-flush-port

switchport-backup startup-active-port-selection

Enables the active port locking function at device startup.

Syntax

To set information:

   switchport-backup startup-active-port-selection primary-only

To delete information:

   no switchport-backup startup-active-port-selection

Input mode

`(config)`

Parameters

primary-only

   Sets only the primary port as the active port at device startup.

   1. Default value when this parameter is omitted:

      This parameter cannot be omitted.

   2. Range of values:

      None

Default behavior

The secondary port can also be selected as the active port at device startup.

Impact on communication

None

When the change is applied

The change is operational as soon as the setting value is changed and every time the device starts.

Notes

1. Even when this configuration has been deleted, the uplink port on which the active port locking function at device startup is running enters a state in which no active ports are set until link-up occurs on the primary port.

2. On the uplink port on which the active port locking function at device startup is running, the function to fix the active port is released if the following conditions exist:

   • Link-up occurs on the primary port.
   • An operation command is used to specify the active port as a secondary port.

Related commands

None

35 L2 Loop Detection

loop-detection

Sets the port type for the L2 loop detection function.

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)`

> Ethernet interface, port channel interface

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 device 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 device 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 device 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 to be exempted from L2 loop detection. When an L2 loop detection frame is received, this will be ignored.
>
> 1. Default value when this parameter is omitted:
>
>> This parameter cannot be omitted.
>
> 2. Range of values:
>
>> None

Default behavior

The port serves as a detecting port. If an L2 loop detection frame is not sent and an L2 loop detection frame sent from the local device 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 function.

Syntax

To set information:

loop-detection enable

To delete information:

no loop-detection enable

Input mode

`(config)`

Parameters

None

Default behavior

The L2 loop detection function 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 retention 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 retention time elapses without another L2 loop detection frame being received, the number of L2 loop detection frames received until the port is deactivated 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 retention 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 this command is set, and the hold time for the number of L2 loop detection frames received has not yet expired, the hold time is reset and the new value takes effect.

Related commands

loop-detection enable

loop-detection interval-time

Sets the sending interval of 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 sending interval (in seconds) of 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 sending interval of 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

36 Storm Control

storm-control

Configures the storm control function.

Syntax

To set or change information:

> storm-control broadcast level pps <packet/s>
>
> storm-control multicast level pps <packet/s>
>
> storm-control unicast level pps <packet/s>

To set information:

> storm-control action inactivate
>
> storm-control action trap
>
> storm-control action log

To delete information:

> no storm-control broadcast
>
> no storm-control multicast
>
> no storm-control unicast
>
> no storm-control action inactivate
>
> no storm-control action trap
>
> no storm-control action log

Input mode

`(config-if)`

> Ethernet interface

Parameters

broadcast

> Sets broadcast frames as subject to storm control.
>
> > 1. Default value when this parameter is omitted:
> >
> > Broadcast frames are excluded from the storm control function.

multicast

> Sets multicast frames as subject to storm control.
>
> > 1. Default value when this parameter is omitted:
> >
> > Multicast frames are excluded from the storm control function.

unicast

> Sets unicast frames as subject to storm control.
>
> > 1. Default value when this parameter is omitted:
> >
> > Unicast frames are excluded from the storm control function.

level pps <packet/s>

> Specifies the allowable reception rate for storm control. Frames exceeding the reception rate are discarded. If 0 is set, all applicable frames are discarded.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 150000000

action inactivate

Deactivates the port when a storm is detected. When this parameter has been specified and a port is de-activated after a storm is detected, a message is always output regardless of the action log settings. Accordingly, it is not necessary to set an action log. The action trap settings are applied when SNMP notifications are sent.

1. Default value when this parameter is omitted:

   If a storm is detected, only the frames exceeding the reception rate are discarded. The port status does not change.

action trap

Sends an SNMP notification when a storm or the end of a storm is detected.

1. Default value when this parameter is omitted:

   No SNMP notification is sent when a storm is detected.

action log

Outputs an operation message when a storm or the end of a storm is detected.

1. Default value when this parameter is omitted:

   No operation 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. Storm control is controlled by the number of received frames. Frame length is irrelevant.

2. When the received frame rates exceed the set reception rate, control frames are also discarded. To prevent necessary control frames from being discarded, do not specify too small a value.

3. With action inactivate, if the port on which a storm is detected belongs to a channel group, deactivates all ports belonging to the channel group. On the other hand, even if a storm occurs on a port for which storm control is not set, storm control is not performed on any ports belonging to a channel group. Also, in a stack configuration, only ports belonging to a channel group in the same member switch as the port on which a storm is detected are deactivated. Therefore, when setting storm control on a port belonging to a channel group, set storm control for all ports belonging to the channel group.

4. If the reception rate is not set for storm-control broadcast, storm-control multicast, or storm-control unicast, the action specified with storm-control action is not performed.

5. 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.

Related commands

None

37 Port Mirroring

monitor session

Configures port mirroring. A maximum of four session numbers of this command and the "destination session" command can be set for each device.

Syntax

To set or change information:

monitor session <session no.> source interface <interface id list> [{rx | tx | both}] destination interface <interface type> <interface number> [encapsulation dot1q <vlan id>]

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. The session number specified with the "destination session" command cannot be specified.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 4

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:

See the following table.

Table 37-1: Setting range for port mirroring

Session number	Setting range	Remarks
1 to 3	rx, tx, both	both is set by default.
4	rx	rx must always be specified.

destination interface <interface type> <interface number>

Specifies a mirror port for port mirroring. If the encapsulation dot1q parameter is not set, the port for which Layer 2 information is set cannot be specified.

<interface type> <interface number>

Specifies an interface for which a mirror port is set.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

- Ethernet interface

encapsulation dot1q <vlan id>

Attaches a VLAN tag with the specified VLAN ID to frames to be mirrored. The VLAN ID specified by the "vlan" command and the "interface vlan" command cannot be specified.

1. Default value when this parameter is omitted:

No VLAN tag is attached.

2. Range of values:

2 to 4094

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. A port that has already been set as a monitor port cannot be set as a monitor port or a mirror port.

2. When policy-based mirroring is set, the port mirroring setting (tx/both) for mirroring sent frames cannot be configured.

3. In a session where the encapsulation dot1q parameter is set, VLAN tags are attached to frames to be mirrored, even if a monitor port is changed or added.

4. For a port on which a VXLAN subinterface is set, when specifying the port as a mirror port, use the encapsulation dot1q parameter to specify a VLAN ID different from the VLAN ID set for the subinterface.

5. For a port on which tag translation is set, when specifying the port as a mirror port, use the encapsulation dot1q parameter to specify a VLAN ID different from the value specified for the VLAN tag of tag translation.

Related commands

None

38 Policy-based Mirroring

destination session

Specifies a mirror port for policy-based mirroring. A maximum of four session numbers of this command and the "monitor session" command can be set for each device.

Syntax

To set or change information:

destination session <session no.> interface <interface type> <interface number>

To delete information:

no destination session <session no.>

Input mode

`(config-dest-mirror)`

Parameters

<session no.>

Specifies a session number for policy-based mirroring. The session number specified with the "monitor session" command cannot be specified.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

1 to 4

interface <interface type> <interface number>

Specifies an interface to be used as a mirror port.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

For <interface type><interface number>, the interface name and interface number corresponding to the following interface type groups can be specified. For details, see "■How to specify the interface" in "Specifiable values for parameters".

- Ethernet interface

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 this command is set, the setting (tx, both) of the port mirroring function cannot be configured to mirror sent frames.

Related commands

None

destination-interface-list

Sets the destination interface list.

Syntax

To set or change information:

destination-interface-list <destination interface list name> mode mirror

To delete information:

no destination-interface-list <destination interface list name> mode mirror

Input mode

`(config)`

Parameters

<destination interface list name>

Sets the destination interface list name.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specifies the destination interface list name with up to 31 characters.

For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

destination session

39 sFlow Statistics

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 "Configuration Guide Vol. 2, 21.1.3(2)(c) Extended data format".

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.

No flow samples in any extended data format are to be sent to the collector.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

Flow samples in any extended data format are sent to the collector.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Any new setting of this command overwrites the old setting. If you want to change a parameter, enter all the necessary parameter values at the same time when you set this command.

Related commands

None

sflow forward egress

Samples sent traffic on the specified port for flow samples and monitors sent and received traffic for counter samples.

Syntax

To set information:

sflow forward egress

To delete information:

no sflow forward egress

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can specify either sflow forward egress or sflow forward ingress for the device. To include sent traffic in the monitoring target for flow samples, delete any sflow forward ingress commands set for other ports, and then set sflow forward egress for a port to be monitored.

Related commands

sflow forward ingress

sflow forward ingress

Samples received traffic on the specified port for flow samples and monitors sent and received traffic for counter samples.

Syntax

To set information:

sflow forward ingress

To delete information:

no sflow forward ingress

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can specify either sflow forward ingress or sflow forward egress for the device. To include received traffic in the monitoring target for flow samples, delete any sflow forward egress commands set for other ports, and then set sflow forward ingress for a port to be monitored.

Related commands

sflow forward egress

sflow max-header-size

Sets the maximum size from the beginning of the sample packet to be copied if the header type is used for the basic data format (see the "sflow packet-information-type" command).

Syntax

To set or change information:

> sflow max-header-size <bytes>

To delete information:

> no sflow max-header-size

Input mode

`(config)`

Parameters

<bytes>

> If the header type is used for the basic data format, this parameter sets the maximum size to be copied (in bytes), starting from the beginning of the sample packet.
>
>   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) assigned to 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 "Configuration Guide Vol. 2, 21.1.3(2)(b) Basic data format".

　　1. Default value when this parameter is omitted:

　　　This parameter cannot be omitted.

　　2. Range of values:

　　　None

Default behavior

Flow samples are sent to the collector in header type format.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow polling-interval

Specifies the interval for sending counter samples to the collector.

Syntax

To set or change information:

sflow polling-interval <seconds>

To delete information:

no sflow polling-interval

Input mode

`(config)`

Parameters

<seconds>

Specifies the interval for sending counter samples to the collector (in seconds). If 0 second is specified, counter samples are not sent to the collector.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

0 to 2147483647 (=2^31-1)

Default behavior

Counter samples are sent to the collector in every 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If 20 or more ports are monitored, the load on the 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 proba-bility 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. Recommended sampling interval values are shown in the "Sampling interval to be used as a guideline" corresponding to the total PPS in " Table 39-1: Reference sampling interval values in the operating environment". If you set a sampling interval that is significantly smaller than the recommended value, the load on the CPU might be exces-sive.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, 2097152

Specify a value that can be obtained from 2^n, where n = 8 to 21. If a value other than these values is entered, one of these values is automatically set depending on the entered value. "Table 39-2: 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 39-1: Reference sampling interval values in the operating environment

Total PPS	Sampling interval to be used as a guideline	Example configuration to be used as a guideline
Up to 25 kpps	256	
Up to 50 kpps	512	100-Mbit/s Ethernet x 1
Up to 100 kpps	1024	
Up to 200 kpps	2048	
Up to 400 kpps	4096	1-Gbit/s Ethernet x 1
Up to 800 kpps	8192	

Total PPS	Sampling interval to be used as a guideline	Example configuration to be used as a guideline
Up to 1.6 Mpps	16384	
Up to 3.2 Mpps	32768	
Up to 6.4 Mpps	65536	10-Gbit/s Ethernet x 1
Up to 13 Mpps	131072	
Up to 26 Mpps	262144	1-Gbit/s Ethernet x 48
Up to 52 Mpps	524288	
Up to 100 Mpps	1048576	
Up to 200 Mpps	2097152	

Table 39-2: Relationship between the entered sampling interval and the sampling interval that is actually set

Sampling interval entered in the command	Sampling interval actually set
256	256
257 to 512	512
513 to 1024	1024
1025 to 2048	2048
2049 to 4096	4096
4097 to 8192	8192
8193 to 16384	16384
16385 to 32768	32768
32769 to 65536	65536
65537 to 131072	131072
131073 to 262144	262144
262145 to 524288	524288
524289 to 1048576	1048576
1048577 to 2097152	2097152
The value must be 2097153 or greater.	2097152

Example:

If 1000 is specified for <sample count>, the value that is actually used is 1024 (= 2^{10}).

Default behavior

The sampling interval applied to the Switch is 2097152 (= 2^{21}).

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 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

Loopback interface IP address for the global network (when using the configuration command)

Priority 2

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

Sets the port number used for HTTP packets to a port number other than 80 when URL information is used in the extended data format.

Syntax

To set or change information:

sflow url-port-add <url port>

To delete information:

no sflow url-port-add

Input mode

`(config)`

Parameters

<url port>

Sets the port number used for HTTP packets to a port number other than 80 when URL information is used in the extended data format.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

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

40 IEEE 802.3ah/UDLD

efmoam active

Sets the port to be monitored by the IEEE 802.3ah/OAM function to active mode.

Syntax

To set or change information:

efmoam active [udld]

To delete information:

no efmoam active

Input mode

`(config-if)`

Ethernet interface

Parameters

udld

Specifies that the port be monitored using the IEEE 802.3ah/UDLD function and enables the unidirectional link failure detection function.

1. Default value when this parameter is omitted:

   The unidirectional link failure detection function is not executed on the applicable port.

2. Range of values:

   None

Default behavior

The applicable port works in passive mode and does not detect a unidirectional link failure.

Impact on communication

If this function 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 function.

Related commands

None

efmoam disable

Enables or disables the IEEE 802.3ah/OAM function on a device.

To disable the IEEE 802.3ah/OAM function, set the "efmoam disable" command.

To enable the IEEE 802.3ah/OAM function 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 function 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

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 function.)

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

41 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 "■Arbitrary 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 lowest 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 function. 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 41-1: Failure descriptions corresponding to the setting values

Setting val-ue	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.

Setting value	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 status.
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 function 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 SNMP notification is sent.

However, if the level of the redetected failure is higher than that of the previously-detected failure, an SNMP notification 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 function 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 function 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 an SNMP notification.

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 from the point at which CC detects a failure until it sends an SNMP notification. 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 time from the point at which CC detects a failure until it sends an SNMP notification is 2500 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 enable

Sets in a domain an MA in which the CC function 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 sending 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 CCM sending interval.

1s

Sets the CCM sending interval to 1 seconds.

10s

Sets the CCM sending interval to 10 seconds.

1min

Sets the CCM sending interval to 1 minutes.

10min

Sets the CCM sending interval to 10 minutes.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

1min is used as the CCM sending interval.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the CCM sending interval 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 work in Up MEP mode.
>
>   1. Default value when this parameter is omitted:
>
>   The Switch works 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 work 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)`

> Ethernet interface, port channel interface

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 a MEP used by the CFM function.

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)

Ethernet interface, port channel interface

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 device) 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:

   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 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 a MIP used by the CFM function.

Syntax

To set information:

ethernet cfm mip level <level>

To delete information:

no ethernet cfm mip level <level>

Input mode

`(config-if)`

Ethernet interface, port channel interface

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 quota-tion 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 "■Arbitrary 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

None

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 specify <vlan id list> and the specifiable range of 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 4094

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

None

42 LLDP

lldp enable

Enables operation of LLDP for a port.

Syntax

To set information:

lldp enable

To delete information:

no lldp enable

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

lldp run

lldp hold-count

Specifies 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 sending 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 sending interval (in seconds) at which the Switch sends LLDP frames.

    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 at which the Switch sends LLDP frames.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

lldp run

lldp management-address

Sets the LLDP management address.

Syntax

To set or change information:

    lldp management-address {ip <ip address> | ipv6 <ipv6 address>}

To delete information:

    no lldp management-address

Input mode

`(config)`

Parameters

{ip <ip address> | ipv6 <ipv6 address>}

    Specify the management address.

      1. Default value when this parameter is omitted:

        This parameter cannot be omitted.

      2. Range of values:

        Specify an IPv4 or IPv6 address.

Default behavior

Neighboring devices are not notified of the management address.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

lldp enable

lldp run

Enables the LLDP function.

Syntax

To set information:

    lldp run

To delete information:

    no lldp run

Input mode

`(config)`

Parameters

None

Default behavior

The LLDP function 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

43 OADP

oadp cdp-listener

Specifies whether the CDP reception function 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 function 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 the OADP function for a port or link aggregation.

Syntax

To set information:

oadp enable

To delete information:

no oadp enable

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Even if this command is set for a port that is a member of a link aggregation, the OADP function does not work. The OADP function 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 specify <vlan id list> and the specifiable range of 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 sending 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) at which the Switch sends OADP frames. 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 sending interval of 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 function.

Syntax

To set information:

oadp run

To delete information:

no oadp run

Input mode

`(config)`

Parameters

None

Default behavior

The OADP function 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

44 PTP

ptp description

Sets supplementary information. This command can be used as a comment about PTP. Note that when this command is set, information can be checked by using the "show ptp operation" command.

Syntax

To set or change information:

ptp description \<string>

To delete information:

no ptp description

Input mode

`(config)`

Parameters

\<string>

Sets a supplementary description of PTP.

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 128 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 "■Arbitrary 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

ptp run

ptp enable

Enables the PTP function for a port.

Syntax

To set information:

ptp enable

To delete information:

no ptp enable

Input mode

(config-if)

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ptp run

ptp run

Enables the PTP function to specify the communication function.

Syntax

To set information:

ptp run e2e-tc

To delete information:

no ptp run

Input mode

`(config)`

Parameters

e2e-tc

Sets the PTP communication function to use E2E-TC.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

None

Default behavior

The PTP function 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

ptp source-interface

Specifies the source VLAN and IP address when sending PTP messages.

Syntax

To set or change information:

> ptp source-interface vlan <vlan id> ip-address <ip address>

To delete information:

> no ptp source-interface vlan <vlan id>

Input mode

`(config)`

Parameters

vlan <vlan id>

> Specifies the VLAN ID of the source VLAN when sending PTP messages.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   See "Specifiable values for parameters".

ip-address <ip address>

> Specifies the IPv4 address when sending PTP messages.
>
> 1. Default value when this parameter is omitted:
>
>   This parameter cannot be omitted.
>
> 2. Range of values:
>
>   Specifies the IPv4 address in dot notation.

Default behavior

The Switch does not send PTP messages.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To send and receive PTP messages, set the configuration to satisfy the following conditions.
   - The <vlan id> specified in this command has been set for an VLAN interface.
   - The <ip address> specified in this command has been set for the above VLAN interface.

Related commands

interface vlan

ip address

ptp run

ptp enable

45 Error Messages Displayed When Editing the Configuration

45.1 Error messages displayed when editing the configuration

45.1.1 Common

Table 45-1: Common error messages

Message	Description
<value1> has already been set -- <value2>.	<value1> information has already been set. <value2> could not be set. Delete <value1> information or check if information you expected is set.
<value1> has already been set.	<value1> information has already been set. Delete <value1> information or check if information you expected is set.
<value1> is not in range from <value2> to <value3>.	The value of the <value1> parameter is outside the valid range. Set a value within the range.
	<value1>: Parameter name <value2>: Minimum value <value3>: Maximum value
Can not change it because data is not corresponding.	Cannot be changed because there is no matching data. Check if information to be changed exists.
Can not delete it because data is not corresponding.	Data cannot be deleted because there is no matching data or duplicated data is specified. Check if there is data to be deleted or duplicated data is specified.
Can't delete this configuration referred by other configuration.	This configuration cannot be changed because it is specified by another configuration. Delete the configuration that refers to this configuration, and then retry the deletion.
Essential parameter <value1> has no value.	Because the <value1> information is a prerequisite condition for a setting that does not exist, the setting cannot be specified. Set the <value1> information.
Interface not found.	The specified interface cannot be found. Check the interface setting.
Invalid DUID. -- <value1>	<value1> is outside the valid DUID range. Set a value within the range.
	<value1>: Invalid value
Invalid IPv4 address. -- <value1>	<value1> is outside the valid IPv4 address range. Set a value within the range.
	<value1>: Invalid value

Message	Description
Invalid IPv6 address. -- <value1>	<value1> is outside the valid IPv6 address range. Set a value within the range.
	<value1>: Invalid value
Invalid line type.	The line type is invalid. Different line types are set within the same NIF.
Invalid MAC address. -- <value1>	<value1> is outside the valid MAC address range. Set a value within the range.
	<value1>: Invalid value
Invalid nif number. -- <value1>	<value1> is outside the valid NIF number range. Set a value within the range.
	<value1>: Invalid value
Invalid port number. -- <value1>	<value1> is outside the valid port number range. Set a value within the range.
	<value1>: Invalid value
Invalid Mask. -- <value1>	<value1> is outside the valid subnet mask range. Set a value within the range.
	<value1>: Invalid value
Maximum number of entries are already defined (config memory shortage). <value1>	Shared memory for the configuration is full. Delete entries that are no longer needed, execute the "save" command, and then add an entry.
	<value1>: Entry name
Maximum number of entries are already defined. <value1>	An attempt is being made to set a configuration that is larger than the capacity limit or to change a configuration in an environment already at the maximum capacity limit. Delete configurations that are no longer used, and then set the configuration again.
	<value1>: Entry name for the maximum capacity limit
Not found <value1>.	The specified <value1> information could not be found. Check if the <vlaue1> information has been set.
Port is not mounted -- <value1>.	The number of the port which is not mounted is specified. Set the number of the port which is mounted or check the status of the port.
	<value1>: A NIF number or a port number
Syntax error -- <value1>.	The configuration syntax or the value is invalid. Set the configuration again with the correct syntax or value.
	<value1>: Invalid value
The different name is already defined.	A different name is already set.

Message	Description
The number in which list specification is possible is \<value1\>.	The maximum number of specifiable elements is \<value1\>. Check if the number does not exceed the capacity limit.
	\<value1\>: Maximum number of elements that can be specified for a list
The sequence number exceeded the maximum value. Try "resequence" Command.	The sequence number exceeds the maximum value. To specify an entry, execute the "resequence" command, and then specify this entry again.
This configuration has already been set.	This configuration has already been set.
Too long value or illegal format (max \<value1\> characters).	The number of characters exceeds the maximum value (\<value1\>), or an invalid character is contained. Use the determined format.
	\<value1\>: Number of characters that can be entered
Too long value or illegal format (max \<value1\> digit number).	The number of characters you entered exceeds the maximum number of digits (\<value1\>), or an invalid character exists. Use the determined format.
	\<value1\>: Number of digits that can be entered

45.1.2 Configuration editing and operation information

Table 45-2: Error messages displayed while editing and operating configurations

Message	Description
\<process\> is starting. Please try again.	A program is being started. Wait a while, and then re-execute the command.
	\<process\>: Program name
A specified number of interfaces exceeds the limitation.	The interface cannot be set because the number of interfaces exceeds the maximum value.
Cannot change switch \<switch no.\> configuration, because config memory shortage.\<reason\>	The configuration of the member switch cannot be changed because of a shortage of shared memory. Restart the member switch to match the configurations.
	\<switch no.\>: Switch number \<reason\>: Additional information
Can't execute config command, please try again.	A communication error occurred between processes. Wait a while, and then re-execute the command.
Configuration command syntax error.line \<line number\> : "\<error syntax\>"	A configuration command of the source file has a syntax error.
	\<line number\>: Number of lines in a copy file \<error syntax\>: Error syntax
Configuration data cannot temporarily delete. Please try again.	Deletion is not permitted temporarily because the configuration you entered is not completed. Wait a while, and then re-execute the command.

Message	Description
Configuration file is empty.	There are no contents in the configuration.
Connection failed between master switch and switch <switch no.>.	Communication with the member switch failed. The configuration might not be applied to the member switch. Restart the member switch to match the configurations.
	<switch no.>: Switch number
Data transfer failed. (<reason>)	Transferring the configuration file to the remote server failed. Re-execute the command with the debug parameter specified for checking.
	<reason>: Additional information
File format error.	The file format is invalid. Make sure the name of the specified file is correct.
File name is a directory.	A directory name cannot be specified. Specify a file name.
File name too long.	The specified file name is too long. Shorten the file name.
Filename or directory path is too long.	The path to the target is too long. Shorten the path length.
Logical inconsistency occurred.	A conflict occurred in the configuration. Take the following actions. If the following cases do not apply, wait a while, and then re-execute the command. • If you are editing data in a level-2 or level-3 configuration command mode, use the "show running-config" operation command to check whether the command that switched to the target command mode was deleted. • If you interrupted the "end" or "quit (exit)" command by pressing Ctrl + C, and then executed the configuration command, use the "end" command to exit the configuration command mode. • If you execute a configuration command while the device is restarting, re-execute the command after the device is restarted.
No enough parameters.	No parameters are specified. Specify the necessary parameters.
No such file or directory.	The specified file or directory is not found. Specify the correct file name or directory name.
Not enough memory, configuration file is too big.	There is not enough memory to save the configuration because it is too large.
Not enough space on device.	Capacity at the write destination is insufficient. Delete files that are no longer needed.
Now configuration data is changing. Please try again.	The configuration you entered cannot be edited because it is not completed. Wait a while, and then re-execute the command.
Permission denied.	You do not have write permission for the target.

Message	Description
Resource temporarily unavailable.	Resource is temporarily insufficient. Wait a while, and then re-execute the command.
The command execution failed, because another command executing.	The command cannot be executed because it conflicts with a command which is being executed.
The command execution failed, because configuration file is editing.	This command cannot be executed because another user is editing the configuration.
The command execution failed, because configuration file is saving.	No edit command can be executed while saving the configuration.
The command execution failed, because master switch is adding other switch to stack.	The command cannot be executed because a member switch is being added. Wait a while, and then re-execute the command. If the switch does not recover after a while, restart the member switch, and then review the priority of frames sent to a Switch.
The command execution failed, because mismatch found between master switch and switch <switch no.> configuration.	This command cannot be executed because there is a configuration mismatch between the master and the member switches. Restart the member switch to match the configurations.
	<switch no.>: Switch number
The command execution failed, because multiple commands can not execute simultaneously.	Multiple commands cannot be executed concurrently.
The command execution failed, because OS type mismatched.	The command cannot be executed because the software of the member switches making up the stack is different.
The command execution failed, because software version mismatched.	The command cannot be executed because the software versions of the member switches making up the stack are different.
The configuration on the master switch was successfully changed, but the configuration on switch <switch no.> was not changed.<reason>	The configuration of the member switch cannot be changed because a problem occurred in an internal program. Restart the member switch to match the configurations.
	<switch no.>: Switch number <reason>: Additional information
The master switch was successfully saved, but the configuration on switch <switch no.> was not saved.	The configuration of the master switch was successfully saved, but that of other member switches failed to be saved. Wait a while, and then re-execute the command.
	<switch no.>: Switch number
The saving command is being executed, please try again.	The operation is not permitted because the "save" command is being executed. Wait a while, and then re-execute the command.
This configuration is active.	This configuration matches the implementation and cannot be changed.

45.1.3 Stack information

Table 45-3: Stack function error messages

Message	Description
Cannot change switchport mode in forty-gigabitethernet interface.	The switchport mode cannot be changed on the fortygigabitethernet interface. Only switchport mode stack can be set.
Cannot delete this command, because up-link redundant configuration specified.	This command cannot be deleted because an uplink redundancy configuration is specified. Delete the setting of the "switchport backup interface" command.
In a stack configuration, only one interface can set the ring-port of the same ring-id to one switch.	A ring port with the same ring ID can only be set for one of the member switches that configure a stack. Set an interface of another member switch as the second ring port. To set another interface of the same member switch as a ring port, first delete the ring port that has already been set.
no service ipv6 dhcp is necessary for stack enable.	Setting stack enable requires no service ipv6 dhcp.
Relations between stack enable and axrp health-check holdtime configuration are inconsistent.	stack enable and axrp health-check holdtime (15 ms to 499 ms) cannot be set simultaneously.
Relations between stack enable and axrp health-check interval configuration are inconsistent.	stack enable and axrp health-check interval (5 ms to 199 ms) cannot be set simultaneously.
Relations between stack enable and axrp mac-clear-mode configuration are inconsistent.	stack enable and axrp mac-clear-mode cannot be set simultaneously.
Relations between stack enable and bfd configuration are inconsistent.	stack enable and BFD cannot be set simultaneously.
Relations between stack enable and cfm configuration are inconsistent.	stack enable and CFM cannot be set simultaneously.
Relations between stack enable and channel group number are inconsistent.	The relations between stack enable and the channel group number are inconsistent. If link aggregation using the channel group number 49 or higher is specified, the stack function cannot be deleted. If the stack function is not used, link aggregation using the channel group number 49 or higher cannot be set.
Relations between stack enable and dot1x system-auth-control are inconsistent.	stack enable and dot1x system-auth-control cannot be set simultaneously.
Relations between stack enable and gsrp configuration are inconsistent.	stack enable and GSRP cannot be set simultaneously.
Relations between stack enable and igmp snooping configuration are inconsistent.	When setting stack enable and IGMP snooping at the same time, set swrt_multicast_table to use IPv4 multicasting together.
Relations between stack enable and ip dhcp snooping are inconsistent.	stack enable and ip dhcp snooping cannot be set simultaneously.
Relations between stack enable and ipv6 multicast-routing are inconsistent.	stack enable and ipv6 multicast-routing cannot be set simultaneously.

Message	Description
Relations between stack enable and mac-authentication system-auth-control are inconsistent.	stack enable and mac-authentication system-auth-control cannot be set simultaneously.
Relations between stack enable and mld snooping configuration are inconsistent.	stack enable and MLD snooping cannot be set simultaneously.
Relations between stack enable and netconf are inconsistent.	stack enable and netconf cannot be set simultaneously.
Relations between stack enable and oadp configuration are inconsistent.	stack enable and OADP cannot be set simultaneously.
Relations between stack enable and part of Ring Protocol configurations are inconsistent.	stack enable and the following Ring Protocol configurations cannot be set simultaneously. • "axrp virtual-link" command • shared-edge parameter of the "axrp-ring-port" command • ring-attribute rift-ring-edge parameter of the "mode" command • monitor-enable parameter of the "multi-fault-detection mode" command
Relations between stack enable and power-control configurations are inconsistent.	stack enable and the configuration of the power saving function cannot be set simultaneously.
Relations between stack enable and ptp configuration are inconsistent.	stack enable and PTP cannot be set simultaneously.
Relations between stack enable and rmon configuration are inconsistent.	stack enable and RMON cannot be set simultaneously.
Relations between stack enable and service dhcp are inconsistent.	stack enable and service dhcp cannot be set simultaneously.
Relations between stack enable and sFlow configuration are inconsistent.	stack enable and sFlow statistics cannot be set simultaneously.
Relations between stack enable and vlan <vlan id> mac-based are inconsistent.	stack enable and MAC VLAN cannot be set simultaneously.
	<vlan id>: VLAN ID
Relations between stack enable and vlan id 4094 are inconsistent.	stack enable and vlan id 4094 cannot be set simultaneously.
Relations between stack enable and VRRP configuration are inconsistent.	stack enable and VRRP cannot be set simultaneously.
Relations between stack enable and web-authentication system-auth-control are inconsistent.	stack enable and web-authentication system-auth-control cannot be set simultaneously.
Relations between switchport mode stack and access-group are inconsistent.	switchport mode stack and any of the following access group commands cannot be set on the same port: • ip access-group • ipv6 traffic-filter • mac access-group

Message	Description
Relations between switchport mode stack and authentication configuration are inconsistent.	switchport mode stack and Layer 2 authentication cannot be set on the same port.
Relations between switchport mode stack and axrp-primary-port are inconsistent.	switchport mode stack and axrp-primary-port cannot be set on the same port.
Relations between switchport mode stack and axrp-ring-port are inconsistent.	switchport mode stack and axrp-ring-port cannot be set on the same port.
Relations between switchport mode stack and CFM configuration are inconsistent.	switchport mode stack and the CFM command cannot be set on the same port.
Relations between switchport mode stack and channel-group mode are inconsistent.	switchport mode stack and channel-group mode cannot be set on the same port.
Relations between switchport mode stack and dot1x configuration are inconsistent.	switchport mode stack and IEEE 802.1X cannot be set on the same port.
Relations between switchport mode stack and efmoam active are inconsistent.	switchport mode stack and efmoam active cannot be set on the same port.
Relations between switchport mode stack and gsrp configuration are inconsistent.	switchport mode stack and the GSRP command cannot be set on the same port.
Relations between switchport mode stack and ip arp inspection trust are inconsistent.	switchport mode stack and ip arp inspection trust cannot be set on the same port.
Relations between switchport mode stack and ip dhcp snooping trust are inconsistent.	switchport mode stack and ip dhcp snooping trust cannot be set on the same port.
Relations between switchport mode stack and ip verify source are inconsistent.	switchport mode stack and ip verify source cannot be set on the same port.
Relations between switchport mode stack and lacp port-priority are inconsistent.	switchport mode stack and lacp port-priority cannot be set on the same port.
Relations between switchport mode stack and lldp configuration are inconsistent.	switchport mode stack and LLDP cannot be set on the same port.
Relations between switchport mode stack and loop-detection are inconsistent.	switchport mode stack and loop-detection cannot be set on the same port.
Relations between switchport mode stack and mac-authentication configuration are inconsistent.	switchport mode stack and MAC-based authentication cannot be set on the same port.
Relations between switchport mode stack and monitor session source interface are inconsistent.	The port specified with switchport mode stack cannot be specified as the monitor port for port mirroring.
Relations between switchport mode stack and part of ethernet configurations are inconsistent.	switchport mode stack and any of the following Ethernet commands cannot be set on the same port: • duplex • link debounce • link up-debounce • mtu • speed

Message	Description
Relations between switchport mode stack and qos-flow-group are inconsistent.	switchport mode stack and any of the following QoS flow group commands cannot be set on the same port: • ip qos-flow-group • ipv6 qos-flow-group • mac qos-flow-group
Relations between switchport mode stack and qos-queue-group are inconsistent.	switchport mode stack and qos-queue-group cannot be set on the same port.
Relations between switchport mode stack and spanning-tree configuration are inconsistent.	switchport mode stack and a command of Spanning Tree Protocols cannot be set on the same port.
Relations between switchport mode stack and storm-control are inconsistent.	switchport mode stack and storm-control cannot be set on the same port.
Relations between switchport mode stack and switchport backup are inconsistent.	switchport mode stack and an uplink port cannot be set on the same port.
Relations between switchport mode stack and traffic-shape rate are inconsistent.	switchport mode stack and traffic-shape rate cannot be set on the same port.
Relations between switchport mode stack and vxlan pmtu are inconsistent.	switchport mode stack and vxlan pmtu cannot be set on the same port.
Relations between switchport mode stack and web-authentication configuration are inconsistent.	switchport mode stack and Web authentication cannot be set on the same port.
stack enable is necessary for switchport mode stack.	Setting switchport mode stack requires stack enable.
switchport mode stack can be set to only fortygigabitethernet interface or hundredgigabitethernet interface.	switchport mode stack can be set only for the fortygigabitethernet or hundredgigabitethernet interface.
switchport mode stack cannot be set more than four ports per one switch.	switchport mode stack can be set for up to four ports per member switch.
switchport mode stack is not supported in this port.	switchport mode stack cannot be set on this port. The command can be set only for any of the 37th through 44th, and 49th through 52nd interfaces.

45.1.4 Login security and RADIUS/TACACS+ information

Table 45-4: Error messages related to login security and RADIUS/TACACS+

Message	Description
Maximum number of entries are already defined. <value1>	You are trying to add more than the allowable maximum number of entries. Delete entries that are no longer needed, and then add the entries.
	<value1>: Entry name
Port Number is duplicate between auth port and acct port.	The port numbers for auth-port and acct-port are the same.

45.1.5 SSH information

Table 45-5: SSH error messages

Message	Description
ssh: '<file path>' file open error.(<reason>)	The specified file cannot be opened.
	<file path>: The specified file <reason>: Error type
ssh: input file is bad format.	The input file format is invalid.
ssh: Public keys are a maximum of 10 entries per one user.	The maximum number of entries of public keys is 10 per user.
ssh: The number of bits of a public key is out of range.	The number of bits of a public key is out of range.
ssh: The public key is bad format.	The public key format is invalid.
ssh: The public key is nothing.	A public key cannot be found.
ssh: The public key is too long.	The public key is too long.
ssh: Usernames are a maximum of 20 entries.	The maximum number of entries of user names is 20.

45.1.6 Host names and DNS information

Table 45-6: Error messages related to host names and DNS

Message	Description
Same name <value> has already been set.	The same name (<value>) has already been set.

45.1.7 Device management information

Table 45-7: Device management error messages

Message	Description
Cannot change the switch model.	The device model cannot be changed.
Cannot configure switch <switch no.> provision configuration because stack is active.	The specified switch number cannot be configured because it is running in stack mode. Check the switch number.
	<switch no.>: Switch number
Can't delete this command, because stack relation configuration specified.	This command cannot be deleted because a stack-related configuration is specified. Delete the stack-related configuration.
Can't edit the configuration, because stack enable configuration specified.	The configuration cannot be edited because stack enable is specified. Set the configuration after restarting the device.
stack enable is necessary for this command.	Setting this command requires the "stack enable" command. Set the "stack enable" command, and then set this command.
The system interface hundredgigabitethernet cannot be set because specified switch model does not support system interface hundredgigabitethernet.	The specified switch model cannot be set because it does not support the system interface hundredgigabitethernet configuration.
This command cannot be set because it will disable the interface used by 'monitor session'	An interface to be disabled when the "system interface hundredgigabitethernet" command is set is set by the "monitor session" command. Delete the setting of the "monitor session" command and then try again.

45.1.8 Power saving function information

Table 45-8: Eror messages related to the power saving function

Message	Description
Relations between "end-time" and "start-time" are inconsistent.	The schedule cannot be set because a date and time earlier than the start date and time is specified for the end date and time. Check the start date and time and the end time for schedule-power-control time-range.

45.1.9 SNMP information

Table 45-9: 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>: Group name
Informs is supported by only SNMPv2C.	The inform function is supported by SNMPv2C. Select SNMPv2C to use the inform function.

Message	Description
Invalid oid-tree. <oid tree>	The value for <oid tree> is invalid. For <oid tree>, specify an object identifier in dot notation.
	<oid tree>: 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>: 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>: MIB view name <oid tree>: Subtree information

45.1.10 Advanced script information

Table 45-10: Advanced script error messages

Message	Description
The cron syntax is invalid.	The cron syntax is invalid. Check the syntax.
The event monitoring is already configured.	Event monitoring has already been set.
The file name extension is invalid.	The script file name extension is invalid. Register a file with one of the following extensions: ".py", ".pyc", and ".pyo".
The specified script id is already configured. (script id = <script id>)	The specified script ID has already been used. Delete the setting of the specified script ID or use an unused script ID for <script id>, and then try again.
	<script id>: The specified script ID
The specified sequence number is already configured. (sequence = <sequence>)	The specified action sequence number has already been used. Delete the setting of the specified action sequence number or use an unused action sequence number for <sequence>, and then try again.
	<sequence>: Action sequence number
The sysmsg syntax is invalid. (interface id = <interface id>)	The syntax of the operation message monitoring is invalid. Check the syntax.
	<interface id>: Details of the specified message type

Message	Description
The sysmsg syntax is invalid. (message text = <message text>)	The syntax of the operation message monitoring is invalid. Check the syntax.
	<message text>: The specified message text

45.1.11 Ethernet information

Table 45-11: Ethernet error messages

Message	Description
'network-clock input-source' cannot be set, because specified port is already set by other input-source.	The specified port cannot be set because it has already been used.
'network-clock input-source' cannot be set, because specified priority is already set for the same switch number.	The specified priority cannot be set because it has already been used by a device with the same number.
'network-clock input-source' cannot be set, because specified switch model does not support Sync-E.	Sync-E cannot be set because the specified switch model does not support it.
A subinterface cannot be set because a channel-group is already set for the port.	A subinterface cannot be set because the port is belonging to a channel group. To specify a subinterface, specify a port that is not belonging to a channel group.
A subinterface cannot be set because a switchport is already set for the Ethernet port.	A subinterface cannot be set because switchport has already been set for the Ethernet port. To specify a subinterface, specify an interface for which no switchport is set.
A switchport cannot be set because a subinterface is already set for the Ethernet port.	switchport mode cannot be set because a subinterface has already been set for the Ethernet port. To set switchport, specify an interface for which no subinterface is set, or delete the subinterface.
Cannot attach the interface specified as a ring-port to the channel-group.	The interface set as a ring port cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete the ring-related configuration.
Cannot attach the interface that specified cfm enable to the channel-group.	The interface for which CFM is set to enable cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete enable for CFM.
Cannot attach the interface that specified mep to the channel-group.	The interface for which MEP is set cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete MEP.
Cannot attach the interface that specified mip to the channel-group.	The interface for which MIP is set cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete MIP.

Message	Description
Cannot attach the interface that specified ptp enable to the channel-group.	The interface for which PTP is set to enable cannot participate in the port channel. To allow the interface to participate in the port channel, first delete enable for PTP.
The number of interfaces exceeds the maximum number for this device.	The number of interfaces exceeded the maximum capacity limit for the Switch. Check the settings in the device and delete unused subinterfaces.
this command is different from this one in channel-group port.	The configured command and the port channel configuration do not match. Match the configuration of the port channel to the configuration of the command.

45.1.12 Link aggregation information

Table 45-12: Link aggregation error messages

Message	Description
A channel group cannot be set because a subinterface is already set for the port.	A channel group cannot be set because a subinterface has already been set for the Ethernet port. Delete the subinterface or set the channel group for another Ethernet port.
A subinterface cannot be set because a channel group is not set.	A subinterface cannot be set because a channel group has not been set.
A subinterface cannot be set because a switchport is already set for the channel group.	A subinterface cannot be set because switchport is set for the channel group. To specify a subinterface, specify an interface for which no switchport is set.
A switchport cannot be set because a subinterface is already set for the channel group.	switchport cannot be set because a subinterface has already been set for the channel group. To set switchport, specify an interface for which no subinterface is set, or delete the subinterface.
Can not change channel-group mode.	The channel group mode cannot be changed. To change it, you must specify multiple ports to delete channel group mode, and then set it again.
Can not delete interface of channel-group because specified port status is up.	The port cannot be deleted because shutdown is not set on some ports. Use the configuration to shut down the applicable ports.
Channel-group <value1> has already been set -- <value2> cannot be set.	The same mode cannot be set under the same interface. <value1>: Channel group you have set <value2>: Channel group you attempted to set
Maximum number of channel-group port are already defined.	No more ports can be set. Review the number of ports for each channel group.
Relations between interface of channel-group and tpid and jumbo_frame in port configuration are inconsistent.	Information about the interface for which channel-group is set and the interface for which tpid and jumbo_frame are set is inconsistent.

Message	Description
The different kind of channel-group mode has already been set -- <mode> cannot be set.	The mode of the channel group which is currently set cannot be changed.
	<mode>: Mode you attempted to set
The number of interfaces exceeds the maximum number for this device.	The number of interfaces exceeded the maximum capacity limit for the Switch. Check the settings in the device and delete unused subinterfaces.
this command is different from this one in channel-group port.	Different settings were found on ports specified for the same channel group. The configuration of the ports specified for the same channel group must either match or be deleted.

45.1.13 MAC address table information

Table 45-13: MAC address table error messages

Message	Description
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	The mac-address-table static VLAN specification and the switchport configuration do not match. A VLAN set by using mac-address-table static must be specified for switchport access or switchport trunk allowed vlan of the interface that has been set.
The configuration cannot be set because the specified VLAN ID has not been configured. (VLAN ID = <vlan id>)	The specified VLAN ID has not been set. Check if the target VLAN exists.
	<vlan id>: VLAN ID

45.1.14 VLAN information

Table 45-14: VLAN error messages

Message	Description
Can not change mode from <value1> to <value2>.	The VLAN type cannot be changed to <value2> because it is already specified as <value1>. To change the VLAN type to the specified one, delete the target VLAN and then try again.
	<value1>, <value2>: VLAN type • port-based: Port VLAN • protocol-based: Protocol VLAN • mac-based: MAC VLAN
Cannot change vlan configuration referred by flow configuration.	The specified vlan configuration cannot be changed because it is specified by a filter or the QoS configuration. To change the specified vlan configuration, delete the filter or the QoS configuration set for the specified vlan configuration first.
Cannot change vlan configuration referred by QoS configuration.	The VLAN configuration cannot be changed. The port type cannot be set because the parameter that uses VLAN tunneling is set in the QoS flow list for the Ethernet interface you have set. Delete the QoS flow list for the Ethernet interface, and then specify the port type.

Message	Description
Cannot delete protocol referred by VLAN configuration.	You are trying to specify a protocol name to be deleted by using the "protocol" command of the VLAN.
	Delete the "protocol" command specification, and then delete the protocol name.
Can't delete vlan <vlan id> configuration referred by <value1> configuration.	The specified VLAN cannot be deleted because it is used by another configuration.
	<vlan id>: VLAN ID
	<value1>: Configuration for which VLAN is set
Can't set <value1> which is not configured to use vlan <vlan id>.	The specified VLAN ID has not been set.
	<value1>: Configuration for which VLAN ID is set
	<vlan id>: VLAN ID
Duplicate translated-tag.	The specified translated ID is being used by another VLAN.
	Check the following:
	• The same translated ID is not used by another VLAN.
	• The VLAN ID for which allowed-vlan is specified, but translated-tag is not specified is not specified.
Inconsistency is found between the mac-based-vlan static-only and the dot1x configuration.	An IEEE 802.1X command cannot be executed when the "mac-based-vlan static-only" command has been executed.
Inconsistency is found between the mac-based-vlan static-only and the web-authentication configuration.	The Web authentication start command cannot be executed when the "mac-based-vlan static-only" command has been executed.
Maximum number of TPID value which can be used is exceeded.	Too many TPID values are specified.
Maximum number which can be used is exceeded.	A maximum of 16 protocol values (ethertype value, llc value, and snap-ethertype value) are used in the entire device. No more than 16 VLANs can be set.
Mirror port and switchport are inconsistent.	The following types of ports cannot be set as mirror ports for sessions that do not use the 802.1Q tagging function for port mirroring.
	• Port other than the access port
	• Port for which tag translation is enabled
	• Port that is belonging to a VLAN or channel group
	Also, the following types of ports cannot be set as mirror ports for sessions that use the 802.1Q tagging function for port mirroring. Additionally, you cannot configure VLAN settings associated with these ports.
	• Protocol port
	• MAC port
	• Stack port
Not found VLAN-ID <vlan id>.	The specified VLAN ID is not set.
	<vlan id>: VLAN ID

Message	Description
Relations between access-list and dot1q-tunnel are inconsistent.	A tunneling port cannot be set on the device because an access list is set on the outbound side of the VLAN interface or because an access list that contains a VLAN ID as a detection condition is set on the outbound side. The tunneling port settings and the following settings cannot be specified simultaneously: • An access list that is applied to the outbound side of the VLAN interface • An access list that contains a VLAN ID as a detection condition and that is applied to the outbound side Delete the tunneling port setting or apply an access list that does not contain a VLAN ID as a detection condition to the Ethernet interface.
Relations between access-list and vlan mapping are inconsistent.	Tag translation cannot be set for the Ethernet interface because an access list that contains a VLAN ID as a detection condition is set on the outbound side of the Ethernet interface. Tag translation cannot be set if an access list that contains a VLAN ID as a detection condition is applied to the outbound side. Delete the tag translation setting or specify an access list that does not contain a VLAN ID as a detection condition.
	Tag translation cannot be set for the Ethernet interface because an access list is set on the outbound side of the VLAN interface. Tag translation cannot be set if an access list is applied to the outbound side. Delete the tag translation setting, or do not apply an access list to the outbound side.
Relations between igmp snooping and l2-isolation are inconsistent.	The IGMP snooping function and the Layer 2 forwarding block function cannot be set concurrently.
Relations between mac-based and vlan-tunneling-enable are inconsistent.	MAC VLANs and VLAN tunneling cannot be set concurrently.
Relations between mld snooping and l2-isolation are inconsistent.	The MLD snooping function and the Layer 2 forwarding block function cannot be set concurrently.
Relations between protocol-based and vlan-tunneling-enable are inconsistent.	A protocol VLAN and VLAN tunneling cannot be set concurrently.
Relations between vlan in dot1q configuration and default vlan are inconsistent.	The default VLAN cannot be set for the "switchport mac dot1q vlan" command (except when a native VLAN is set).
Relations between vlan in dot1q configuration and mac vlan configuration are inconsistent.	switchport mac dot1q vlan and switchport mac vlan cannot be set because they use the same VLAN.
Relations between vlan in dot1q configuration and native configuration are inconsistent.	switchport mac dot1q vlan and switchport mac native vlan cannot both be configured because they specify the same VLAN.
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	The mac-address-table static VLAN specification and the switchport configuration do not match. A VLAN set by using mac-address-table static must be specified for switchport access or switchport trunk allowed vlan of the interface that has been set.

Message	Description
Relations between vlan-tunneling and IP configuration are inconsistent.	VLAN tunneling information and IP information are inconsistent. When VLAN tunneling is set, IP information cannot be set.
The following items conflict: the switch-port mode and the policy-based mirror port.	The following types of ports cannot be set as mirror ports for policy-based mirroring. • Port other than the access port • Port for which tag translation is enabled • Port for which a VLAN is set
The maximum number of vlan-mac entries are exceeded.	The number of MAC address entries for each VLAN exceeds the capacity limit. Up to 128 MAC address entries can be set for each VLAN.
The VLAN cannot be set because it is referred by port mirroring configuration.	The specified VLAN cannot be set because it is specified for port mirroring.
The VLAN ID cannot be deleted because it is referred by 'no mac-address-table learning'. (VLAN ID = <vlan id>)	The specified VLAN ID cannot be deleted because it is used for the MAC address learning suppression setting. Delete the configuration that refers to this configuration, and then retry the deletion.
	<vlan id>: VLAN ID
VLAN is not MAC VLAN.	A VLAN specified by switchport mac vlan is not a MAC VLAN. Specify a MAC VLAN.
VLAN is not Port VLAN.	The specified VLAN is not a port VLAN. Specify a port VLAN.
VLAN is not Protocol VLAN.	A VLAN specified by switchport protocol vlan is not a protocol VLAN. Specify a protocol VLAN.

45.1.15 VXLAN information [SL-L3A]

Table 45-15: VXLAN error messages

Message	Description
Cannot delete loopback interface referred by source-interface configuration.	A loopback interface cannot be deleted because it is set with the source-interface configuration. Delete the setting with the "no source-interface loopback" command before entering the command.
Destination ip address is already configured in other vtep.	The destination IP address has already been used by another VTEP.
Invalid vni list.	The specified VNI list is invalid.
Not found loopback interface.	The specified loopback interface has not been configured. Configure the loopback interface before entering the command.
Relations between vxlan and igmp snooping configuration are inconsistent.	VXLANs and IGMP snooping cannot be used concurrently.
Relations between vxlan and mld snooping configuration are inconsistent.	VXLANs and MLD snooping cannot be used concurrently.

Message	Description
Relations between vxlan and multicast routing are inconsistent.	VXLANs and the multicast routing function cannot be set concurrently.
Relations between vxlan and policy based routing are inconsistent.	VXLANs and policy-based routing cannot be set concurrently.
Relations between vxlan and vlan mapping are inconsistent.	VXLANs and tag translation cannot be set concurrently.
Relations between vxlan and vlan-tunneling-enable are inconsistent.	VXLANs and VLAN tunneling cannot be set concurrently.
Source interface is already configured in other vtep.	The source interface has already been used by another VTEP.
The configuration cannot be set because the specified VNI has not been configured. (VNI = <vni>)	The specified VNI has not been set. Check if the VNI specified in the "member vni" command exists.
	<vni>: VNI
The maximum number of destination ip address entries are exceeded.	The number of registered destination IP addresses exceeds the upper limit.
The maximum number of vni entries exceeded.	The number of registered VNIs exceeds the upper limit.
The VNI cannot be deleted because it is referred by 'no mac-address-table learning'. (VNI = <vni>)	The specified VNI cannot be deleted or changed because it is used in the MAC address learning suppression setting. Delete the configuration that refers to this configuration, and then retry the deletion.
	<vni>: VNI
The vxlan pmtu cannot be set because the maximum number of TCP/UDP port entries are exceeded.	The number of TCP/UDP port number detection patterns cannot be set because it exceeds the capacity limit. Make changes to satisfy the capacity limit and then try again.
VLAN ID <vlan id> is already configured in other subinterface.	The VLAN ID you are trying to set has already been set for another subinterface of the same physical interface or channel group. Specify a different VLAN ID.
	<vlan id>: VLAN ID (not displayed for untagged frames)
Vni is already configured in other vtep.	The VNI number has already been used by another VTEP.
Vni is already configured in other.	The VNI you are trying to set has already been used by another VTEP. Check if the VNI is duplicated in VLANs and subinterfaces.

45.1.16 Spanning Tree information

Table 45-16: Spanning Tree error messages

Message	Description
Can not configure spanning-tree when gsrp is configured.	The Spanning Tree Protocol cannot be set because GSRP is set.

Message	Description
Cost is over 65535, please set up in 1 to 65535 or set pathcost method to long.	The value for cost is equal to or greater than 65535. Set the cost value from 1 to 65535 or set long for pathcost method.
Maximum number of MST instance are already defined.	The number of MST instances has already reached the maximum number. The maximum number of MST instances that can be set is 16.
Pathcost method is short, please set up in 1 to 65535 or set pathcost method to long.	short is set for pathcost method. Set the cost value from 1 to 65535 or set long for pathcost method.
Relations between PVST+ and the protocol-vlan or mac-vlan configuration are inconsistent.	PVST+ and a protocol VLAN or a MAC VLAN cannot be set concurrently.
Relations between vlan-tunneling and spanning-tree configuration are inconsistent.	The VLAN tunneling configuration does not match the Spanning Tree configuration. When a VLAN tunneling configuration is set, the Spanning Tree Protocol must be stopped.
spanning-tree: maximum number of MST instance are already defined.	The number of MST instances has already reached the maximum number. The maximum number of MST instances that can be set is 16.

45.1.17 Ring Protocol information

Table 45-17: Ring Protocol error messages

Message	Description
axrp-<ring id>-<group id>: vlan-mapping <mapping id> is already configured in another vlan-group.	The specified VLAN mapping has already been set for a VLAN group in the same ring. Either delete the VLAN mapping from another VLAN group or use another VLAN mapping.
	<ring id>: Ring ID <group id>: VLAN group ID <mapping id>: VLAN mapping ID
axrp-<ring id>: cannot configure this command to channel-group port.	A ring port cannot be set for an interface that is participating in a port channel.
	<ring id>: Ring ID
axrp-<ring id>: cannot configure this command to port channel interface for channel group that consists of ports of multiple switches.	A ring port cannot be set for a port channel interface of a channel group in which ports of multiple member switches are registered.
	<ring id>: Ring ID
axrp-<ring id>: maximum number of ring-id are already defined.	The maximum number of ring IDs that can be used in a device is 24. No more than 24 VLANs can be set. To add a ring ID, you must first delete a registered ring ID.
	<ring id>: Ring ID
axrp-<ring id>: maximum number of ring-port are already defined.	Set two ring ports for each ring ID. To set another port as a ring port, first delete a ring port that has already been set.
	<ring id>: Ring ID

Message	Description
axrp-<ring id>: shared-edge port is already defined in another ring-port.	As for shared ports, shared-edge is already set for another ring port. To set another port as a shared-edge shared port, first delete a shared port that has already been set.
	<ring id>: Ring ID
axrp-<ring id>: this interface is already defined as a ring port of other ring configured the same vlan-mapping.	The specified interface has already been set as a ring port of another ring to which the same VLAN mapping as the ring set by using this command is applied. Set the applicable interface as a shared link or specify another interface.
	<ring id>: Ring ID
axrp-<ring id>: vlan <vlan id> is already configured in control-vlan.	The specified VLAN has already been set in the control VLAN. Either delete the applicable VLAN from the control VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in control-vlan of other ring.	The specified VLAN has already been set in the control VLAN of another ring. Either delete the applicable VLAN from the other ring's control VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in multi-fault-detection-vlan.	The specified VLAN has already been set in the multi-fault monitoring VLAN. Either delete the applicable VLAN from the multi-fault monitoring VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in multi-fault-detection-vlan of other ring.	The specified VLAN has already been set in the multi-fault monitoring VLAN of another ring. Either delete the applicable VLAN from the other ring's multi-fault monitoring VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in virtual-link.	The specified VLAN has already been set for a virtual link. Either delete the applicable VLAN from the virtual link or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID

Message	Description
axrp-<ring id>: vlan <vlan id> is already configured in vlan-mapping.	The specified VLAN has already been set for VLAN mapping. Either delete the applicable VLAN from the VLAN mapping or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan-mapping <mapping id> is already configured in vlan-group of other ring.	The specified VLAN mapping has already been set for a VLAN group in another ring. Either delete the VLAN mapping from the other VLAN group or use other VLAN groups.
	<ring id>: Ring ID <mapping id>: VLAN mapping ID
axrp-virtual-link-<link id>: vlan <vlan id> is already configured in control-vlan.	The specified VLAN has already been set in the control VLAN. Either delete the applicable VLAN from the control VLAN or use another VLAN.
	<link id>: Virtual link ID <vlan id>: VLAN ID
axrp-vlan-mapping-<mapping id>: vlan <vlan id> is already configured in control-vlan.	The specified VLAN has already been set in the control VLAN. Either delete the applicable VLAN from the control VLAN or use another VLAN.
	<mapping id>: VLAN mapping ID <vlan id>: VLAN ID
axrp-vlan-mapping-<mapping id>: vlan <vlan id> is already configured in multi-fault-detection-vlan.	The specified VLAN has already been set in the multi-fault monitoring VLAN. Either delete the applicable VLAN from the multi-fault monitoring VLAN or use another VLAN.
	<mapping id>: VLAN mapping ID <vlan id>: VLAN ID
axrp-vlan-mapping-<mapping id>: vlan <vlan id> is already configured in other vlan-mapping.	The specified VLAN has already been set for another mapping. Either delete the applicable VLAN from the other VLAN mapping or use another VLAN.
	<mapping id>: VLAN mapping ID <vlan id>: VLAN ID
Cannot configure axrp-virtual-link when multi-fault-detection is configured.	A virtual link cannot be set because the multi-fault monitoring function has been set.
Cannot configure multi-fault-detection when axrp-virtual-link is configured.	The multi-fault monitoring function cannot be set because a virtual link has been set.

45.1.18 IGMP snooping information

Table 45-18: IGMP snooping error messages

Message	Description
Maximum number of VLAN are already defined.	The number of VLANs that can be specified by using the IGMP snooping function is 64. No more than 64 VLANs can be set.
Relations between igmp snooping and vlan mapping are inconsistent.	VLAN mapping cannot be specified for a trunk port in a VLAN for which the IGMP snooping function is set.
Relations between igmp snooping and vlan-tunneling are inconsistent.	The IGMP snooping function and VLAN tunneling cannot be specified concurrently.
Relations between igmp/mld snooping and multicast configuration are inconsistent.	If swrt_multicast_table has not been set, multicast and IGMP snooping cannot be used concurrently on the same device. If IGMP snooping is running when a multicast setting is entered, an error occurs.
Relations between IP address and igmp snooping is inconsistent.	ip igmp snooping cannot be set because seven or more IP addresses has been set for the VLAN. Decrease the number of set IP addresses for the VLAN to 6 or less.
Relations between mrouter in igmp snooping configuration and channel-group configuration are inconsistent.	To specify an mrouter by using a channel group number, specify a channel group number that has already been set.
Relations between mrouter in igmp snooping configuration and switchport configuration are inconsistent.	The port or the channel group specified by an mrouter does not belong to the applicable VLAN. Specify the port or the channel group that belongs to the VLAN.

45.1.19 MLD snooping information

Table 45-19: MLD snooping error messages

Message	Description
Maximum number of VLAN are already defined.	The number of VLANs that can be specified by using the MLD snooping function is 32. No more than 32 VLANs can be set.
Relations between igmp/mld snooping and multicast configuration are inconsistent.	If swrt_multicast_table has not been set, multicast and MLD snooping cannot be used concurrently on the same device. If MLD snooping is running when a multicast setting is entered, an error occurs.
Relations between mld snooping and vlan mapping are inconsistent.	VLAN mapping cannot be specified for a trunk port in a VLAN for which the MLD snooping function is set.
Relations between mld snooping and vlan-tunneling are inconsistent.	The MLD snooping function and VLAN tunneling cannot be specified concurrently.
Relations between mrouter in mld snooping configuration and channel-group configuration are inconsistent.	To specify an mrouter by using a channel group number, specify a channel group number that has already been set.
Relations between mrouter in mld snooping configuration and switchport configuration are inconsistent.	The port or the channel group specified by an mrouter does not belong to the applicable VLAN. Specify the port or the channel group that belongs to the VLAN.

45.1.20 Flow detection modes/flow performance information

Table 45-20: Error messages related to flow detection modes/flow performance

Message	Description
Cannot change the configuration because there is an inconsistency between flow detection mode and ip verify source.	A conflict occurred between the terminal filter setting and the flow detection mode setting. To set a terminal filter, specify one of the following flow detection modes: • layer3-dhcp-1 • layer3-suppress-dhcp-1 • Specify dhcp-filter for the flow detection condition of the custom mode.
Cannot change the flow action-change cos.	The priority determination behavior cannot be changed because QoS flow detection conditions and performance information entries are applied to the interface. To change the priority determination behavior, delete all QoS flow detection conditions and performance information entries applied to the interface. Note that you can use the "show system" operation command to check the number of QoS entries used by this configuration file.
Cannot change the configuration because there is an inconsistency between flow detection mode and policy based routing.	A conflict occurred between the policy-based routing setting and the flow detection mode setting. To set the flow detection mode to other than the modes listed below, delete the settings of the "policy-list", "policy-list default-init-interval", and "policy-list default-aging-interval" commands. • layer3-6 • layer3-mirror-3 • layer3-mirror-4 • layer3-mirror-5 • layer3-suppress-2 • layer3-suppress-mirror-2 • custom
Cannot change the flow detection mode.	The flow detection mode cannot be changed because an access list, a QoS flow list, or a terminal filter of DHCP snooping is applied to the interface. To change the flow detection mode, delete all the lists that are applied to the receiving-side interface and the sending-side interface and all terminal filters of DHCP snooping.
Cannot change the flow detection out mode.	The sending-side flow detection mode cannot be changed because an access list is applied to the interface. To change the sending-side flow detection mode, delete all access lists that are applied to the receiving-side interface and the sending-side interface.
Cannot set the flow detection mode because of setting discontiguous entry blocks.	The same flow detection condition for the flow detection mode is not set in multiple consecutive entry blocks. If you specify the flow detection condition of the flow detection mode to be the same for multiple entry blocks, set the condition in consecutive entry blocks.

45.1.21 Access list information

Table 45-21: Access list error messages

Message	Description
Cannot attach this list because flow detection mode layer3-1.	If the receiving-side flow detection mode is layer3-1, the access list cannot be applied.
	If the receiving-side flow detection mode is layer3-1, IPv4 and MAC access lists can be applied.
	To do so, you can use the following commands:
	ip access-group command
	mac access-group command
Cannot attach this list because flow detection mode layer3-2.	If the receiving-side flow detection mode is layer3-2, the access list cannot be applied.
	If the receiving-side flow detection mode is layer3-2, IPv4 access lists can be applied.
	To do so, you can use the following commands:
	ip access-group command
Cannot attach this list because flow detection mode layer3-5.	If the receiving-side flow detection mode is layer3-5, the access list cannot be applied.
	If the receiving-side flow detection mode is layer3-5, IPv4 and IPv6 access lists can be applied.
	To do so, you can use the following commands:
	ip access-group command
	ipv6 traffic-filter command
Cannot attach this list because flow detection mode layer3-6.	If the receiving-side flow detection mode is layer3-6, the access list cannot be applied.
	If the flow detection mode is layer3-6, IPv4 and IPv6 access lists can be applied.
	To do so, you can use the following commands:
	ip access-group command
	ipv6 traffic-filter command
Cannot attach this list because flow detection mode layer3-dhcp-1.	If the receiving-side flow detection mode is layer3-dhcp-1, the access list cannot be applied.
	If the receiving-side flow detection mode is layer3-dhcp-1, an IPv4 access list can be applied.
	To do so, you can use the following commands:
	ip access-group command
Cannot attach this list because flow detection out mode layer3-1-out.	If the sending-side flow detection mode is layer3-1-out, the access list cannot be applied.
	If the sending-side flow detection mode is layer3-1-out, IPv4 access lists can be applied.
	To do so, you can use the following commands:
	ip access-group command
Cannot attach this list because flow detection out mode layer3-2-out.	If the sending-side flow detection mode is layer3-2-out, the access list cannot be applied.
	If the sending-side flow detection mode is layer3-2-out, the access list for which out is specified can be applied.

Message	Description
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, specify for the destination address an IP address that is not a multicast address, restricted broadcast address, or internal loopback 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.
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.
Relations between access-list and dot1q-tunnel are inconsistent.	A tunneling port is set on the device, so an access list cannot be set on the outbound side of the VLAN interface, or an access list that contains a VLAN ID as a detection condition cannot be set on the outbound side.
	The tunneling port settings and the following settings cannot be specified simultaneously:
	• An access list that is applied to the outbound side of the VLAN interface
	• An access list that contains a VLAN ID as a detection condition and that is applied to the outbound side
	Delete the tunneling port setting or apply an access list that does not contain a VLAN ID as a detection condition to the Ethernet interface.
Relations between access-list and vlan mapping are inconsistent.	An access list that contains a VLAN ID as a detection condition cannot be set on the outbound side of the Ethernet interface because tag translation is set for the Ethernet interface.
	Tag translation cannot be set if an access list that contains a VLAN ID as a detection condition is applied to the outbound side.
	Delete the tag translation setting or specify an access list that does not contain a VLAN ID as a detection condition.
	An access list cannot be set on the outbound side of the VLAN interface because tag translation is set for the Ethernet interface.
	Tag translation cannot be set if an access list is applied to the outbound side.
	Delete the tag translation setting, or do not apply an access list to the outbound side.
The destination interface list name cannot be specified.	The destination interface list name cannot be specified.
	Specify the name of an applicable destination interface list that has already been created.

Message	Description
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" operation command. • This entry cannot be set because it is not supported in receiving-side flow detection mode and sending-side flow detection mode. Change the receiving-side flow detection mode and sending-side flow detection mode to ones that allow the specified entry to be set, and then try again.
The maximum number of TCP/UDP port entries are exceeded.	The number of TCP/UDP port number detection patterns exceeds the capacity limit. Make changes to satisfy the capacity limit and then try again.
The number of policy based mirroring entries exceeds the maximum.	• The number of policy-based mirroring entries exceeds the capacity limit. Delete some of the existing entries and then try again. You can use the "show system" operation command to check the number of entries used. • This entry cannot be set because it is not supported in receiving-side flow detection mode and sending-side flow detection mode. Change the receiving-side flow detection mode and sending-side flow detection mode to ones that allow the specified entry to be set, and then try again.
This list cannot be set to the outbound because the list includes TCP/UDP port range entry.	Flow detection conditions in this access list cannot be applied to this interface. A list that does not contain a range of source port numbers or destination port numbers specified in detection conditions can be applied to the sending-side interface. To do so, you can use the following commands: ip access-group command ipv6 traffic-filter command
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 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 port.	This access list cannot be applied to this Ethernet interface. When an access list is applied to an Ethernet interface, the VLAN ID of a flow detection condition in the access list must be included in the settings of the Ethernet interface to which you want to apply the access list.
This list cannot be set to VLAN.	This access list cannot be applied to VLAN interfaces. If the VLAN ID is set as a flow detection condition in an access list, the access list cannot be applied to the VLAN interface. Apply it to an Ethernet interface or delete the VLAN ID from the detection condition.

Message	Description
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.

45.1.22 QoS information

Table 45-22: QoS error messages

Message	Description
Cannot attach this list because flow detection mode layer3-1.	If the receiving-side flow detection mode is layer3-1, the QoS flow list cannot be applied.
	If the receiving-side flow detection mode is layer 3-1, IPv4 QoS and MAC QoS flow lists can be applied.
	To do so, you can use the following commands:
	ip qos-flow-group command
	mac qos-flow-group command
Cannot attach this list because flow detection mode layer3-2.	If the receiving-side flow detection mode is layer3-2, the QoS flow list cannot be applied.
	If the receiving-side flow detection mode is layer3-2, IPv4 QoS flow lists can be applied.
	To do so, you can use the following commands:
	ip qos-flow-group command
Cannot attach this list because flow detection mode layer3-5.	If the receiving-side flow detection mode is layer3-5, the QoS flow list cannot be applied.
	If the receiving-side flow detection mode is layer3-5, IPv4 QoS and IPv6 QoS flow lists can be applied.
	To do so, you can use the following commands:
	ip qos-flow-group command
	ipv6 qos-flow-group command
Cannot attach this list because flow detection mode layer3-6.	If the flow detection mode is layer3-6, the QoS flow list cannot be applied.
	If the flow detection mode is layer3-6, IPv4 QoS and IPv6 QoS flow lists can be applied.
	To do so, you can use the following commands:
	ip qos-flow-group command
	ipv6 qos-flow-group command
Cannot attach this list because flow detection mode layer3-dhcp-1.	If the receiving-side flow detection mode is layer3-dhcp-1, the QoS flow list cannot be applied.
	If the receiving-side flow detection mode is layer3-dhcp-1, an IPv4 QoS flow list can be applied.
	To do so, you can use the following commands:
	ip qos-flow-group command

Message	Description
Conform count is greater than trial count.	The number of bandwidth compliances exceeds the number of times of monitoring. Set the number of bandwidth compliances to a value less than or equal to the number of times of monitoring.
Exceed count is greater than trial count.	The number of bandwidth non-compliances exceeds the number of times of monitoring. Set the number of bandwidth non-compliances to a value less than or equal to the number of times of monitoring.
Min packet rate must be less than max packet rate.	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.
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-packet-burst must be less than max-packet-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.
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.
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.
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 <rate> and <burst size> are inconsistent.	If the value of bandwidth monitoring is 10 G or lower, the burst size cannot be set to 32 M or 64 M. If the value of bandwidth monitoring is 10 G or lower, the burst size can be set to a value from 32 k through 16 M. If the value of bandwidth monitoring exceeds 10 G, the burst size can be set to a value from 32 k through 64 M. For details about the available settings for the burst size, see "26 QoS". <rate>: max-rate or min-rate <burst size>: max-rate-burst or min-rate-burst
Specified burst size of traffic-shape rate is incorrect, or it is out of range.	The burst size specified for port bandwidth control is either incorrect or outside the specifiable range.
Specified min-rate value is out of range.	The specified minimum guaranteed bandwidth exceeds the specified range.

Message	Description
Specified rate value of 4PQ+8WFQ is incorrect.	The specified rate value of 4PQ+8WFQ is incorrect.
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.

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" operation command.
	
	• This entry cannot be set because it is not supported in receiving-side flow detection mode.
	
	  Change the receiving-side flow detection mode to one that allows the specified entry to be set, and then try again.

The maximum number of TCP/UDP port entries are exceeded.	The number of TCP/UDP port number detection patterns exceeds the capacity limit. Make changes to satisfy the capacity limit and then try again.
The total of min-rate exceeded bandwidth of port.	The total of the specified minimum guaranteed bandwidths exceeds the bandwidth. Set the value to be equal to or smaller than the bandwidth.
The total of WFQ min-rate exceeded bandwidth of traffic-shape rate.	The total of the minimum guaranteed bandwidths for the WFQ mode exceeds the bandwidth of port bandwidth control. Set the total of the minimum guaranteed bandwidths for WFQ mode so that the value is equal to or smaller than the bandwidth of port bandwidth control.
This aggregate-policer aggregate name is not defined.	The summarized bandwidth monitoring list name cannot be specified. Specify the name of an applicable summarized bandwidth monitoring list that has already been created.
This list cannot be set to this interface, because the list includes copy-user-priority parameter.	The copy-user-priority parameter in the action specification cannot be applied to this interface. If the copy-user-priority parameter is specified in the action specification in a QoS flow list, apply that QoS flow list to an Ethernet interface with VLAN tunneling configured, or delete this parameter from the action specification.
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 VLAN ID of a flow detection condition in the QoS flow list must be included in the settings of the Ethernet interface to which you want to apply the list.
This list cannot be set to VLAN.	This QoS flow list cannot be applied to VLAN interfaces. If the VLAN ID is set as a flow detection condition in a QoS flow list, the QoS flow list cannot be applied to the VLAN interface. Apply it to an Ethernet interface or delete the VLAN ID from the detection condition.
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.

45.1.23 IEEE 802.1X information

Table 45-23: 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.	VLAN-based authentication (static) 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>: Channel group number
	<vlan id>: 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>: 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>: Channel group number
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>: Channel group number
Inconsistency is found between IGMP snooping and the dot1x multiple-authentication configuration.	IGMP snooping is inconsistent with port-based authentication for which auto is set for new terminal detection mode.
	IGMP snooping cannot be set together with port-based authentication for which auto is set for new terminal detection mode.
Inconsistency is found between IGMP snooping and the dot1x vlan <vlan id> supplicant-detection auto configuration.	IGMP snooping is inconsistent with the configuration of VLAN-based authentication (static) for which auto is set for new terminal detection mode.
	IGMP snooping cannot be set together with VLAN-based authentication (static) for which auto is set for new terminal detection mode.
	<vlan id>: VLAN ID

Message	Description
Inconsistency is found between IGMP snooping and the dot1x vlan dynamic supplicant-detection auto configuration.	IGMP snooping is inconsistent with VLAN-based authentication (dynamic) for which auto is set for new terminal detection mode.
	IGMP snooping cannot be set together with VLAN-based authentication (dynamic) for which auto is set for new terminal detection mode.
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 configuration and the l2protocol-tunnel eap configuration.	The IEEE 802.1X configuration is inconsistent with the EAPOL forwarding configuration.
	The "dot1x system-auth-control" command and the "l2protocol-tunnel eap" command cannot be set simultaneously.
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>: 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 definition" command cannot be set simultaneously.
port <switch no.>/<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.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
	<vlan id>: VLAN ID
port <switch no.>/<nif no.>/<port no.>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	Port-based authentication ports 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.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number

Message	Description
port <switch no.>/<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.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
port <switch no.>/<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.
	<switch no.>/<nif no.>/<port no.>: Switch number/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 VLAN port or MAC VLAN port.
	For a VLAN using VLAN-based authentication (static), you cannot use the "switchport protocol-vlan" or "switchport mac-vlan" command to set a protocol VLAN or MAC VLAN, respectively, as a native VLAN.
	You cannot set VLAN-based authentication (static) for a protocol 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>: 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.
	<vlan id>: 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>: VLAN ID

Message	Description
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>: 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>: 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.

45.1.24 Web authentication information

Table 45-24: 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 vrf and the web-authentication configuration.	The "web-authentication system-auth-control" command and the "vrf definition" command cannot be set simultaneously.
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.

Message	Description
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>: Maximum connection time for Web authentication
Invalid max-user . -- <value>	The maximum number of concurrent users is outside the valid range.
	<value>: 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 4094.
	<value>: VLAN ID of the VLAN after 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>: 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 IGMP snooping and authentication arp-relay configuration are inconsistent.	An ARP forwarding command and IGMP snooping cannot be used concurrently on the same device.
Relations between IGMP snooping and authentication ip access-list configuration are inconsistent.	An authentication access list command and IGMP snooping cannot be used concurrently on the same device.
Relations between IGMP snooping and web-authentication configuration are inconsistent.	Web authentication and IGMP snooping cannot be used concurrently on the same device.
Relations between the authentication force-authorized vlan configuration and the dot1q vlan configuration are inconsistent.	When you specify a post-authentication VLAN in the configuration for forced authentication in dynamic VLAN mode, you cannot set a VLAN ID specified by the "switchport mac dot1q vlan" command.
Relations between the vlan configuration and the authentication force-authorized vlan configuration are inconsistent.	When you specify a post-authentication VLAN in the configuration for forced authentication in dynamic VLAN mode, the VLAN ID you specify must have been registered as 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 VLAN mode.

Message	Description
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 function.

45.1.25 MAC-based authentication information

Table 45-25: MAC-based authentication error messages

Message	Description
Inconsistency is found between the vrf and the mac-authentication configuration.	The "mac-authentication system-auth-control" command and the "vrf definition" command cannot be set simultaneously.
Relations between IGMP snooping and mac-authentication configuration are inconsistent.	MAC-based authentication and IGMP snooping cannot be used concurrently on the same device.
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 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.

45.1.26 DHCP snooping information

Table 45-26: DHCP snooping error messages

Message	Description
Cannot change the configuration because there is an inconsistency between flow detection mode and ip verify source.	A conflict occurred between the terminal filter setting and the flow detection mode setting. To set a terminal filter, specify the following flow detection mode: • layer3-dhcp-1 • layer3-suppress-dhcp-1 • Specify dhcp-filter for the flow detection condition of the custom mode.
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.

45.1.27 GSRP information

Table 45-27: 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>: 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>: GSRP group ID <channel group number>: Channel group number
gsrp-<gsrp group id>: can not specify both any flush methods and direct-link on the port <switch no.>/<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>: GSRP group ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
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>: GSRP group ID <channel group number>: Channel group number
gsrp-<gsrp group id>:can not specify the two or more flush methods on the port <switch no.>/<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>: GSRP group ID <switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
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>: GSRP group ID <vlan group id>: VLAN group ID <vlan id>: VLAN ID

45.1.28 VRRP information

Table 45-28: 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.	A follower virtual router cannot follow other virtual routers. The virtual router specified as a primary virtual router should be configured not to be a follower virtual router.
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.
Cannot specify IPv6 virtual router for Follow virtual router.	An IPv6 virtual router cannot be a follower virtual router.
Cannot specify IPv6 virtual router for Primary virtual router.	An IPv6 virtual router cannot be specified as a primary virtual router.
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.
Follow virtual router cannot become the address owner.	A follower virtual router cannot be set as the address owner. When setting an IP address for an interface, setting a virtual IP address for a follower virtual router, or setting a primary virtual router to be followed, a follower virtual router should be configured not to 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>: 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.

Message	Description
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 exceeded the upper limit.

45.1.29 Uplink redundancy information

Table 45-29: Uplink redundancy error messages

Message	Description
Cannot configure this command to channel-group port.	This command cannot be set for an interface participating in a port channel.
Cannot configure this command to port channel interface for channel group that consists of ports of multiple switches.	Uplink redundancy cannot be set for a port channel interface of a channel group in which ports of multiple member switches are registered.
channel-group <channel group number> is invalid.	The specified channel group has already been specified for an uplink port. The same port is specified as a primary port and a secondary port.
	<channel group number>: Channel group number
Port <switch no.>/<nif no.>/<port no.> is invalid.	The specified port has already been specified for an uplink port. The same port is specified as a primary port and a secondary port.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
Relations between flush-request transmit and mac-address-table update transmit are inconsistent.	The sending of flush control frames and sending of MAC address update frames cannot be set concurrently.
Relations between flush-request transmit and reset-flush-port are inconsistent.	The sending of flush control frames and port resetting cannot be set concurrently.
Relations between reset-flush-port and mac-address-table update transmit are inconsistent.	Port resetting and the sending of MAC address update frames cannot be set concurrently.
Relations between uplink redundant and gsrp are inconsistent.	The uplink redundancy configuration is inconsistent with the GSRP configuration. Uplink redundancy and GSRP cannot be configured concurrently.
Relations between uplink redundant and ring protocol are inconsistent.	The uplink redundancy configuration is inconsistent with the Ring Protocol configuration. Uplink redundancy and the Ring Protocol cannot be configured concurrently on the same post or channel group.
Relations between uplink redundant and spanning-tree are inconsistent.	The uplink redundancy configuration is inconsistent with the Spanning Tree configuration. Uplink redundancy and the Spanning Tree Protocol cannot be configured concurrently.
The uplink redundant cannot be set more than one port per one member switch.	An uplink port can only be set for one of the member switches that configure a stack.

45.1.30 Port mirroring information

Table 45-30: Port mirroring error messages

Message	Description
Mirror port and monitor port are inconsistent.	Both mirror port and monitor port settings cannot be specified for the same port.
Mirror port and policy based mirror port are inconsistent.	You cannot specify the same mirror port as the one specified for policy-based mirroring. Specify a port that is not used for policy-based mirroring.
Mirror port and switchport are inconsistent.	The following types of ports cannot be set as mirror ports for sessions that do not use the 802.1Q tagging function for port mirroring. • Port other than the access port • Port for which tag translation is enabled • Port that is belonging to a VLAN or channel group Also, the following types of ports cannot be set as mirror ports for sessions that use the 802.1Q tagging function for port mirroring. Additionally, you cannot configure VLAN settings associated with these ports. • Protocol port • MAC port • Stack port
Monitor port can specify only in one monitor session.	A monitor port can be specified only in one monitor session.
Outbound mirror port and policy based mirror are inconsistent.	If policy-based mirroring is used, the monitor session setting for mirroring sent frames (both/tx) cannot be configured. When using port mirroring to mirror sent frames (both/tx), delete the policy-based mirroring setting.
The port mirroring VLAN tag cannot be set because it is referred by VLAN configuration.	The VLAN tag for port mirroring cannot be set because it is specified for the VLAN configuration.
The same session number is not usable between port mirroring and policy-based mirror.	The same session number cannot be specified for monitor sessions of policy-based mirroring and port mirroring. Use a different session number than the one used for port mirroring.

45.1.31 Policy-based mirroring information

Table 45-31: Policy-based mirroring error messages

Message	Description
Mirror port and policy based mirror port are inconsistent.	You cannot specify the same mirror port as the mirror port specified for port mirroring. Specify a port that is not used for port mirroring.
Outbound mirror port and policy based mirror are inconsistent.	If monitor session is used to mirror sent frames (both/tx), policy-based mirroring cannot be configured. When using policy-based mirroring, delete the mirroring setting for sent frames of port mirroring.

Message	Description
The destination interface is duplicated.	You cannot specify a mirror port used for other mirror sessions in the destination interface list.
	Specify a mirror port that is not used for other mirror sessions in the destination interface list.
The following items conflict: the policy-based mirror port and the switchport mode.	The following types of ports cannot be set as mirror ports for policy-based mirroring.
	• Port other than the access port
	• Port for which tag translation is enabled
	• Port for which a VLAN is set
The same session number is not usable between policy-based mirror and port mirroring.	You cannot set the same session numbers for mirror sessions of port mirroring and policy-based mirroring.
	Set different session numbers for mirror sessions of port mirroring and policy-based mirroring.
The session number is duplicated.	The session number in use cannot be set.
	Set an unused session number.

45.1.32 sFlow statistics information

Table 45-32: 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.
Only either of the following commands "sflow forward egress" or "sflow forward ingress" can be configured at a time on this device.	You can specify either sflow forward egress or sflow forward ingress for the device.
	To specify the sent traffic as the monitoring target, delete any sflow forward ingress specifications for other ports, and then set the command for the port to be monitored.
	To specify the received traffic as the monitoring target, delete any sflow forward egress specifications for other ports, and then set the command for the port to be monitored.

45.1.33 CFM information

Table 45-33: 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.
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.

Message	Description
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>: 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>: Domain level
MA <no.> is already configured in cfm domain.	The specified MA identification number is already being used by another domain.
	<no.>: MA identification number
MA name <name> is already configured in cfm domain.	The specified MA name is already set in the same domain.
	<name>: 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>: 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>: 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>: VLAN ID

45.1.34 LLDP information

Table 45-34: LLDP error messages

Message	Description
Relations between 'lldp run' and 'l2protocol-tunnel lldp' are inconsistent.	The LLDP function and the LLDP forwarding function cannot be set in the device at the same time.

45.1.35 OADP information

Table 45-35: 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.

45.1.36 PTP information

Table 45-36: PTP error messages

Message	Description
Cannot configure ptp enable to channel-group port.	PTP of an interface participating in a port channel cannot be enabled.