AX2500S Software Manual

Configuration Command Reference

For Version 3.5

AX25S-S003X-70

AlaxalA

Relevant products

This manual applies to the models in the AX2500S series of switches. It also describes the functionality of version 3.5 of the software for the AX2500S series of switches. The described functionality is that supported by the OS-L2B-A/OS-L2B and the advanced software upgrade license (the "License").

Export restrictions

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

Trademarks

Reading and storing this manual

Before you use the equipment, carefully read the manual and make sure that you understand all safety precautions. After reading the manual, keep it in a convenient place for easy reference.

Notes

Information in this document is subject to change without notice.

Editions history

January 2013 (Edition 8) AX25S-S003X-70

Copyright

History of Amendments

Ver. 3.5 (Edition 8)

Summary of amendments

Location and title	**Changes**
1. Reading the Manual	Explanations of the AX2530S-24TD, AX2530S-48TD, and AX2530S-24S4XD were added.
2. Connecting from an Operation Terminal	The explanation of the `line vty` command was changed.
21. Access Lists	A parameter was added to the following commands: ● deny (ip access-list extended) ● deny (ipv6 access-list) ● deny (mac access-list extended) ● permit (ip access-list extended) ● permit (ipv6 access-list) ● permit (mac access-list extended)
22. QoS	A parameter was added to the following commands: ● qos (ip qos-flow-list) ● qos (ipv6 qos-flow-list) ● qos (mac qos-flow-list)
23. Common to Layer 2 Authentication	The `authentication logout linkdown` command was added.
25. Web Authentication	The following commands were added: ● web-authentication redirect polling ● web-authentication redirect queries ● web-authentication redirect target A parameter was added to the `web-authentication jump-url` command.
37. SNMP	A parameter was added to the `snmp-server host` command.
40. LLDP	The `lldp version` command was added.
42. Error Messages Displayed When Editing the Configuration	The error messages for access list information were changed.

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

Ver. 3.4 (Edition 7)

Summary of amendments

Location and title	**Changes**
VLAN	The `switchport mac auto-vlan` command was added. The explanation of the `switchport mac` command was changed.
Common to Layer 2 Authentication	The `authentication auto-logout strayer` command was added.

Location and title	Changes
Web Authentication	The web-authentication prefilter command was added.
sFlow Statistics	This chapter was added.
Error Messages Displayed When Editing the Configuration	The error messages for sFlow statistics were added. The error messages for IEEE 802.1X information were changed.

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

Ver. 3.3 (Edition 6)

Summary of amendments

Location and title	Changes
Login Security and RADIUS	The ipv6 access-class command was added. The parameter was added to the following commands: ● radius-server host ● server The explanation of the ip access-group command was changed.
Host Names and DNS	This chapter was added.
Ethernet	The link up-debounce command was added.
Ring Protocol	The following commands were added: ● axrp virtual-link ● axrp-primary-port ● flush-request-count ● flush-request-transmit vlan ● health-check holdtime ● health-check interval ● multi-fault-detection holdtime ● multi-fault-detection interval ● multi-fault-detection mode ● multi-fault-detection vlan ● preempt-delay The parameter was added to the following commands: ● axrp-ring-port ● mode The explanations of the following commands were changed: ● axrp ● axrp vlan-mapping ● control-vlan ● vlan-group
IPv4, ARP, and ICMP	The arp command was added. The explanation of the ip mtu command was changed.
IPv6, NDP, and ICMPv6	This chapter was added.
IEEE 802.1X	The parameter was added to the dot1x radius-server host

Location and title	Changes
	command.
Web Authentication	The parameter was added to the `web-authentication radius-server host` command.
MAC-based Authentication	The parameter was added to the `mac-authentication radius-server host` command.
SNMP	The parameter was added to the `snmp-server host` command. The explanation of the `snmp-server community` command was changed.
Log Data Output Functionality	The parameter was added to the `logging host` command.
Port Mirroring	The parameter was added to the `monitor session` command.
Error Messages Displayed When Editing the Configuration	The error messages for the IPv6, NDP, and ICMPv6 information were added. The error messages for the following information were changed: ● Common ● VLAN information ● Ring Protocol information ● MLD snooping information ● IPv4, ARP, and ICMP information

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

Ver. 3.2 (Edition 5)

Summary of amendments

Location and title	Changes
Ethernet	The explanations of the following commands were changed: ● mtu ● system mtu
VLANs	The following commands were added: ● switchport dot1q ethertype ● switchport vlan mapping ● switchport vlan ● vlan-dot1q-ethertype The parameter was added to the `switchport mode` command. The explanations of the following commands were changed: ● switchport access ● vlan
Access Lists	The explanations of the following commands were changed: ● ip access-group ● ipv6 traffic-filter ● mac access-group

Location and title	Changes
Error Messages Displayed When Editing the Configuration	The error messages for the following information were changed: ● Common ● VLAN information ● Spanning Tree information ● IGMP snooping information ● MLD snooping information ● IEEE 802.1X information ● DHCP snooping information ● CFM information

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

Ver. 3.2 (Edition 4)

Summary of amendments

Location and title	Changes
Reading the Manual	Explanations of the AX2530S-24T4X and AX2530S-48T2X were added.
Login Security and RADIUS	The explanation of the `ip access-group` command was changed.
Device Management	The explanations of the following commands were changed: ● system fan mode ● system temperature-warning-level ● system temperature-warning-level average
Power Saving Functionality	The explanations of the following commands were changed: ● schedule-power-control wakeup-option ● system fan-control
Ethernet	The explanations of the following commands were changed: ● duplex (gigabitethernet) ● speed (gigabitethernet)
Flow Detection Mode	The parameter was added to the following commands: ● flow detection mode ● flow detection out mode

Location and title	Changes
Access Lists	The following commands were added: ● deny (ipv6 access-list) ● ipv6 access-list ● ipv6 access-list resequence ● ipv6 traffic-filter ● permit (ipv6 access-list) The explanations of the following commands were changed: ● deny (ip access-list extended) ● deny (ip access-list standard) ● deny (mac access-list extended) ● ip access-group ● ip access-list extended ● ip access-list resequence ● ip access-list standard ● mac access-group ● mac access-list extended ● mac access-list resequence ● permit (ip access-list extended) ● permit (ip access-list standard) ● permit (mac access-list extended) ● remark
QoS	The following commands were added: ● ipv6 qos-flow-group ● ipv6 qos-flow-list ● ipv6 qos-flow-list resequence ● qos (ipv6 qos-flow-list) The explanations of the following commands were changed: ● ip qos-flow-group ● ip qos-flow-list ● ip qos-flow-list resequence ● mac qos-flow-group ● mac qos-flow-list ● mac qos-flow-list resequence ● qos (ip qos-flow-list) ● qos (mac qos-flow-list) ● remark
MAC-based Authentication	The explanation of the `mac-authentication access-group` command was changed.
SML (Split Multi Link) [OS-L2A]	The explanation of the `system sml peer-link` command was changed.
SNMP	The explanation of the `snmp-server community` command was changed.
Error Messages Displayed When Editing the Configuration	The error messages for the following information were changed: ● Common ● VLAN information ● Access list information ● QoS information

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

Ver. 3.1 (Edition 3)

Summary of amendments

Location and title	**Changes**
Login Security and RADIUS	The `aaa authentication login end-by-reject` command was added.
Device Management	The `system temperature-warning-level average` command was added.
Power Saving Functionality	The explanation of the `schedule-power-control wakeup-option` command was changed.
Ethernet	The explanations of the following commands were changed: ● duplex ● flowcontrol ● speed
IGMP Snooping	The `ip igmp snooping fast-leave` command was added.
Web Authentication	The `aaa authentication web-authentication end-by-reject` command was added.
MAC-based Authentication	The `aaa authentication mac-authentication end-by-reject` command was added.
SNMP	The following commands were added: ● snmp-server engineID local ● snmp-server group ● snmp-server user ● snmp-server view The parameter was added to the `snmp-server host` command. The explanations of the following commands were changed: ● rmon event ● snmp-server community
Error Messages Displayed When Editing the Configuration	The error messages for SNMP information were changed.

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

Ver. 3.1 (Edition 2)

Summary of amendments

Location and title	**Changes**
Device Management	The following commands were added: ● system fan mode ● system temperature-warning-level
Power Saving Functionality	The explanations of the following commands were changed: ● power-control port cool-standby ● schedule-power-control port cool-standby ● schedule-power-control wakeup-option

Location and title	Changes
Ethernet	The `interface tengigabitethernet` command was added. The explanations of the following commands were changed: ● bandwidth ● duplex ● flowcontrol ● interface gigabitethernet ● link debounce ● mdix auto ● mtu ● shutdown ● speed ● system mtu
MAC Address Table	The parameter was added to the `mac-address-table static` command.
Spanning Tree Protocol	The explanations of the following commands were changed: ● spanning-tree pathcost method ● spanning-tree single pathcost method ● spanning-tree vlan pathcost method
IGMP Snooping	The parameter was added to the `ip igmp snooping mrouter` command.
MLD Snooping	The parameter was added to the `ipv6 mld snooping mrouter` command.
QoS	The range of values for the *<Min rate>* parameter of the `qos-queue-list` command was changed. The parameter was added to the `traffic-shape rate` command.
Uplink Redundancy	The parameter was added to the `switchport backup interface` command.
SML (Split Multi Link) [OS-L2A]	The explanation of the `system sml peer-link` command was changed.
Port Mirroring	The parameter was added to the `monitor session` command.
Error Messages Displayed When Editing the Configuration	The error messages for the following information were changed: ● Ethernet information ● QoS information ● Web authentication information ● SML (Split Multi Link) information

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

Preface

Applicable products and software versions

This manual applies to the models in the AX2500S series of switches. It also describes the functionality of version 3.5 of the software for the AX2500S series of switches. The described functionality is that supported by the OS-L2B-A/OS-L2B and the advanced software upgrade license (the "License").

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

Unless otherwise noted, this manual describes the functionality applicable commonly to AX2500S series switches. The functionalities specific to each model are indicated as follows:

[24T]:

The description applies to the AX2530S-24T switch.

[24T4X]:

The description applies to the AX2530S-24T4X switch.

[48T]:

The description applies to the AX2530S-48T switch.

[48T2X]:

The description applies to the AX2530S-48T2X switch.

[24S4X]:

The description applies to the AX2530S-24S4X switch.

[24TD]:

The description applies to the AX2530S-24TD switch.

[48TD]:

The description applies to the AX2530S-48TD switch.

[24S4XD]:

The description applies to the AX2530S-24S4XD switch.

[10G model]:

The description applies to AX2530S-24T4X, AX2530S-48T2X, AX2530S-24S4X, and AX2530S-24S4XD switches.

Unless otherwise noted, this manual describes the functionality for OS-L2B-A/OS-L2B. Functionality related to the Software License Agreement and License Sheet is indicated as follows:

[OS-L2A]:

The description indicates functionality supported by the Software License Agreement and License Sheet.

Corrections to the manual

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

Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

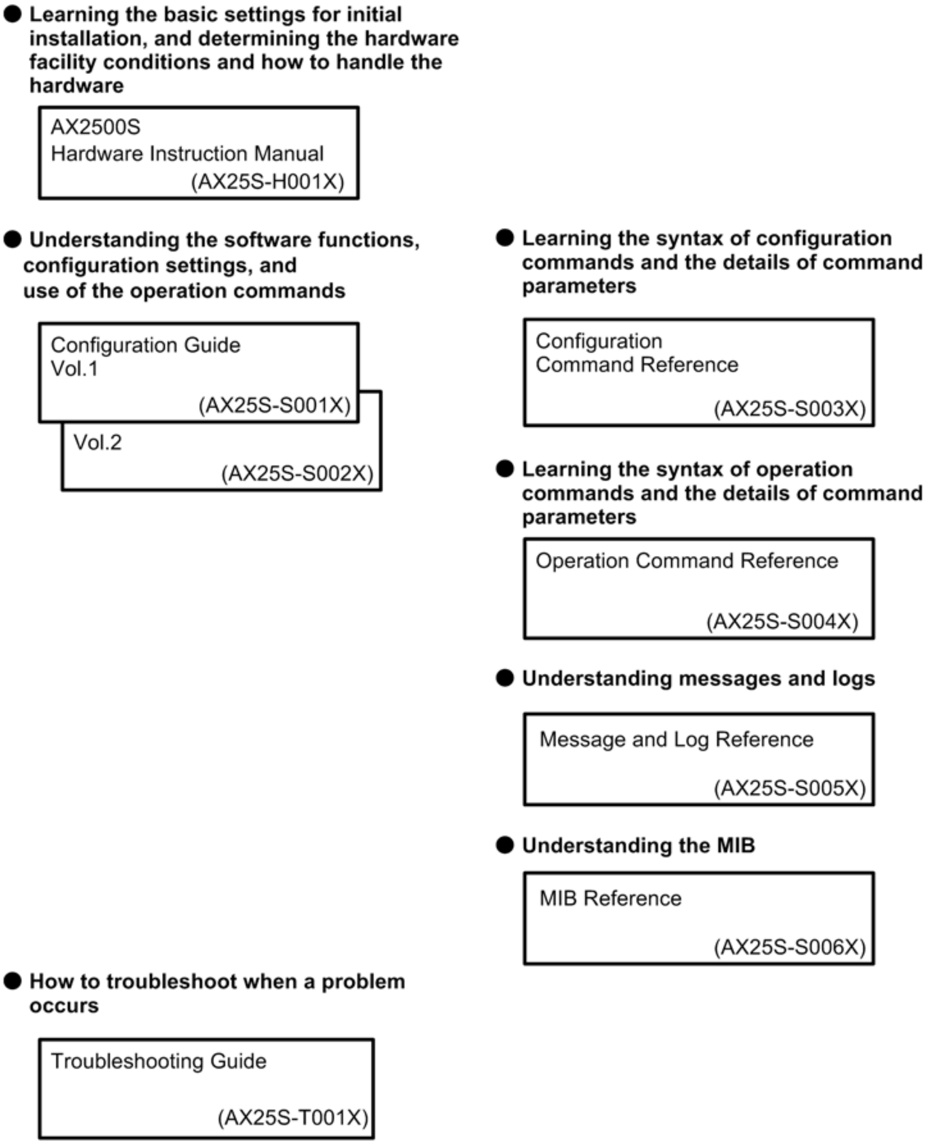
Manual URL

You can view this manual on our website at:

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

Reading sequence of the manuals

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



- **Learning the basic settings for initial installation, and determining the hardware facility conditions and how to handle the hardware**

  AX2500S Hardware Instruction Manual (AX25S-H001X)

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

  Configuration Guide Vol.1 (AX25S-S001X)

  Vol.2 (AX25S-S002X)

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

  Configuration Command Reference (AX25S-S003X)

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

  Operation Command Reference (AX25S-S004X)

- **Understanding messages and logs**

  Message and Log Reference (AX25S-S005X)

- **Understanding the MIB**

  MIB Reference (AX25S-S006X)

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

  Troubleshooting Guide (AX25S-T001X)

Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
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
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
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol

E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
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
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast

PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
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
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
SML	Split Multi Link
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
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier

TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

Conventions: The terms "Switch" and "switch"

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

- AX2500S 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.

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

1 KB (kilobyte) is 1024 bytes.

1 MB (megabyte) is 1024^2 bytes.

1 GB (gigabyte) is 1024^3 bytes.

1 TB (terabyte) is 1024^4 bytes.

Contents

Part 1: Reading the Manual

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 by using the name displayed in the prompt.

Parameters

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

Default behavior

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

Impact on communication

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

When the change is applied

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

Notes

Provides cautionary information on using the command.

Related commands

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

Command mode list

The following table lists the command modes.

Table 1-1 Command mode list

#	Command mode name	Description	Command for mode transition
1	(config)	Global configuration mode	> enable # configure
2	(config-line)	Configures remote login and console.	(config)# line vty (config)# line console
3	(config-group)	Configures a RADIUS server group.	(config)# aaa group server radius
4	(config-if)	Configures an interface.	(config)# interface
5	(config-if-range)	Configures multiple interfaces.	(config)# interface range
6	(config-vlan)	Configures VLAN.	(config)# vlan
7	(config-mst)	Configures Multiple Spanning Tree.	(config)# spanning-tree mst configuration
8	(config-axrp)	Configures the Ring Protocol.	(config)# axrp
9	(config-ext-nacl)	Configures an IPv4 packet filter.	(config)# ip access-list extended
10	(config-std-nacl)	Configures an IPv4 address filter.	(config)# ip access-list standard
11	(config-ipv6-acl)	Configures an IPv6 filter.	(config)# ipv6 access-list
12	(config-ext-macl)	Configures a MAC filter.	(config)# mac access-list extended
13	(config-ip-qos)	Configures IPv4 QoS.	(config)# ip qos-flow-list
14	(config-ipv6-qos)	Configures IPv6 QoS.	(config)# ipv6 qos-flow-list
15	(config-mac-qos)	Configures MAC QoS.	(config)# mac qos-flow-list
16	(dhcp-config)	Configures the DHCP server.	(config)# ip dhcp pool
17	(config-auto-cf)	Configures AUTOCONF.	(config)# auto-config
18	(config-netconf)	Configures NETCONF.	(config)# netconf
19	(config-ether-cfm)	Configures the domain name and MA.	(config)# ethernet cfm domain

Specifiable values for parameters

The following table describes the values that can be specified for parameters. If there are no limitations on parameter names, see *Any character string*.

Table 1-2 Specifiable values for parameters

Parameter type	Description	Input example
Any character string	See *List of character codes*.	name "PORT BASED VLAN-1"
Access list name QoS flow list name	See *List of character codes*. The first character must be an alphabetical character. Subsequent characters can be alphanumeric characters, hyphens (`-`), underscores (`_`), and periods (`.`). It is possible to enter other characters, but use only the characters mentioned above. In addition, do not specify a character string, `resequence`, or a character string beginning with `resequence`.	mac access-list extended list101
QoS queue list name DHCP address pool name	See *List of character codes*. The firtst character must be an alphabetical character. Subsequent characters can be alphanumeric characters, hyphens (`-`), underscores (`_`), and periods (`.`). It is possible to enter other characters, but use only the characters mentioned above.	ip dhcp pool floorA
Host name	You can use alphanumeric characters, hyphens (`-`), and periods (`.`). However, you cannot specify the following characters: ● Period (`.`) for the first character ● Successive periods (`..`) ● Only with numerics and periods (`.`) Note that the maximum of 63 characters can be entered between periods (`.`).	ip host telnet-host 192.168.1.1
MAC address, MAC address mask	Specify these items in hexadecimal format, separating 2-byte hexadecimal values by periods (`.`).	1234.5607.08ef 0000.00ff.ffff
IPv4 address, IPv4 net mask	Specify these items in decimal format, separating 1-byte decimal values by periods (`.`).	192.168.0.14 255.255.255.0
IPv4 address wildcard	The same input format as IPv4 addresses. Setting a bit indicates permission.	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

Parameter type	Description	Input example
Specification of multiple interfaces	Set the information about multiple interfaces. Specifiable interfaces are gigabitethernet, tengigabitethernet, vlan, and port-channel. You can specify gigabitethernet and tengigabitethernet interfaces at the same time, but cannot specify any other interfaces at the same time. The following are the input formats: ● For gigabitethernet interface range gigabitethernet *<interface id list>* ● For tengigabitethernet interface range tengigabitethernet *<interface id list>* ● For vlan interface range vlan *<VLAN ID list>* ● For port-channel interface range port-channel *<Channel group# list>* You can specify no more than 8 of the above input formats, separating each by a comma (`,`).	interface range gigabitethernet 0/1-3 interface range tengigabitethernet 0/25-26 interface range vlan 1-100
add/remove specification	Add to or delete from the information when multiple interfaces have been specified. The add specification adds information to the current information. The remove specification deletes information from the current information. When the add and remove specifications are used, if the `show` command displays duplicated information, delete the duplicated information to optimize the information. The following shows an optimization example of information when multiple interfaces are specified: ● Information before entering a command: switchport trunk allowed vlan 100,101 ● Input command: switchport trunk allowed vlan add 103 ● Information after entering a command: switchport trunk allowed vlan 100,101,103	switchport trunk allowed vlan add 100,200-210 switchport trunk allowed vlan remove 100,200-210 switchport isolation interface add gigabitethernet 0/1-3 switchport isolation interface remove gigabitethernet 0/1-3

<IF#> Parameter range

Specify the *<IF#>* parameter in the format *NIF No./Port No.* (include the last period). *NIF No.* of the Switch is fixed at zero.

The following tables list the range of *<IF#>* values.

Table 1-3 Range of <IF#> values

#	Model	Ethernet type	Range of values
1	AX2530S-24T/AX2530S-24TD	gigabitethernet	0/1 to 0/28
2	AX2530S-24T4X	gigabitethernet	0/1 to 0/24
		tengigabitethernet	0/25 to 0/28
3	AX2530S-48T/AX2530S-48TD	gigabitethernet	0/1 to 0/52
4	AX2530S-48T2X	gigabitethernet	0/1 to 0/50
		tengigabitethernet	0/51 to 0/52
5	AX2530S-24S4X/AX2530S-24S4XD	gigabitethernet	0/1 to 0/24
		tengigabitethernet	0/25 to 0/28

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

If *<interface id list>* is written in parameter input format, use a hyphen (-) or commas (,) to specify multiple interfaces of the type gigabitethernet or tengigabitethernet. You can also specify one gigabitethernet interface and tengigabitethernet interface, in the same way as when *<IF#>* is written in parameter input format. The range of specifiable values is the same as the range of *<IF#>* values in the above table.

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

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

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

The following table describes the range for the *<VLAN ID>* and *<vlan id>* value.

Table 1-4 Range of <VLAN ID> and <vlan id> values

#	Range of values
1	1 to 4094

How to specify <VLAN ID list> /<vlan id list>and the range of values that can be set

If *<VLAN ID list>* or *<vlan id list>* is written in parameter input format, use a hyphen (-) or commas (,) to specify multiple VLAN IDs. You can also specify one VLAN ID, as when *<VLAN ID>* or *<vlan id>* is written as the parameter input format. The range of values that can be set is the same as the range of *<VLAN ID>* or *<vlan id>* values above.

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

1-3,5,10

Range of values that can be set for <Channel group#>

The following tables list the range of *<Channel group#>* values.

Table 1-5 Range of <Channel group#> values

#	Model	Range of values
1	All models	1 to 64

How to specify <Channel group# list> and the range of specifiable values

If *<Channel group# list>* is written in parameter input format, use a hyphen (`-`) or commas (`,`) to specify multiple channel group numbers. You can also specify one channel group number, as when *<Channel group#>* is written. The range of specifiable values is the same as the range of *<Channel group#>* values above.

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

1-3,5

List of character codes

Character codes are listed in the following table.

Characters other than alphanumeric characters in the following list of character codes are special characters.

Table 1-6 List of character codes

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

#1: To enter this character in a character string, you must enclose the entire character string in double quotation marks (").

#2: Use this character to enclose an entire character string. You cannot enter it as part of a character string.

Part 2: Operation and Management of Switches

2. Connecting from an Operation Terminal

ftp-server
line console
line vty
speed
transport input

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

To delete information:

no ftp-server

Input mode

`(config)`

Parameters

None

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

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.

Related commands

line vty

ip access-group

ipv6 access-class

line console

Entering this command changes the mode to config-line mode, which permits settings related to the specified CONSOLE (RS232C) port.

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 Telnet remote access to a switch. This command is also used to limit the number of remote users that can be simultaneously logged in to the switch.

Syntax

To set or change information:

line vty *<start allocation>* *<end allocation>*

To delete information:

no line vty

Input mode

`(config)`

Parameters

<start allocation>

Sets permission for remote login.

- Default value when this parameter is omitted:

  This parameter cannot be omitted.
- Range of values:

  0 (fixed)

<end allocation>

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 access that uses the Telnet protocol.

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 access using the Telnet protocol from any remote operation terminal to be accepted. To restrict access, see *8.1.7 Setting the IP addresses of remote operation terminals permitted to log in* in the manual *Configuration Guide Vol. 1* 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.

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.

Syntax

To set or change information:

transport input {telnet | all | none}

To delete information:

no transport input

Input mode

`(config-line)`

Parameters

{telnet | all | none}

telnet

Accepts remote access that uses the Telnet protocol.

all

Accepts remote access using any protocol (currently only Telnet is supported).

none

Does not accept remote access using any protocol.

1. Default value when this parameter is omitted:

   `all` (Accepts remote access that uses the Telnet protocol.)

2. Range of values:

   `telnet`, `all`, or `none`.

Default behavior

Accepts remote access that uses the Telnet protocol.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

Related commands

line vty

ftp-server

ip access-group

ipv6 access-class

transport input

3. Editing and Working with Configurations

end

Ends configuration command mode and returns you to administrator mode.

Syntax

end

Parameters

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 would be lost when the machine goes to sleep! Do you exit "configure" without save ? (y/n):	When the following commands are configured, configuration command mode will end without any changes being saved: ● schedule-power-controlsystem-sleep ● schedule-power-control time-range The configuration changes you made will be lost when the Switch switches to sleep mode. Enter `y` to finish editing. Enter `n` to cancel the `end` command. If necessary, use the `save` command to save the edited configuration.
The machine is just going to sleep! Do you exit ? (y/n):	If configuration command mode ends, the Switch will switch to sleep mode. Enter `y` to switch to the sleep state. If you do not want to switch to the sleep state, enter `n` to cancel the `end` command, and then use the `(config)# $set power-control schedule disable` command to set the power saving schedule functionality to suppression mode. Note that if the `schedule-power-control wakeup-option linkup` command is set, the Switch will not switch to the sleep mode until the specified interfaces change to a link-down state.

Notes

1. You can use the `end` command to temporarily exit configuration command mode without saving configuration file changes to internal flash memory. If you do so, the editing process of the configuration file will still be incomplete, so save the file after you finish making changes.
2. After editing the running configuration, if you execute the `end` command without saving the changes to internal flash memory, the startup configuration file in internal flash memory and the running configuration will not be the same. After editing the configuration, you must always save your changes.

Related commands

None

exit

Returns to the previous mode. If you are editing data in config mode, this command ends configuration command mode and returns you to administrator mode. If you are editing data in subcommand mode, you are returned one level higher.

Syntax

exit

Parameters

None

Response messages

The following table describes the response messages for the `exit` command.

Table 3-2 Response messages for the exit command

Message	Description
Unsaved changes would be lost when the machine goes to sleep! Do you exit "configure" without save ? (y/n):	When the following commands are configured, configuration command mode will end without any changes being saved: ● schedule-power-control system-sleep ● schedule-power-control time-range The configuration changes you made will be lost when the Switch switches to sleep mode. Enter `y` to finish editing. Enter `n` to stop the `exit` command. If necessary, use the `save` command to save the edited configuration.
The machine is just going to sleep! Do you exit ? (y/n):	If configuration command mode ends, the Switch will switch to sleep mode. Enter `y` to switch to the sleep state. If you do not want to switch to the sleep state, enter `n` to cancel the `exit` command, and then use the `(config)# $set power-control schedule disable` command to set the power saving schedule functionality to suppression mode. Note that if the `schedule-power-control wakeup-option linkup` command is set, the Switch will not switch to the sleep mode until the specified interfaces change to a link-down state.

Notes

Note the following if you use the `exit` command in `config` mode:

1. You can use the `exit` command to temporarily exit configuration command mode without saving configuration file changes to internal flash memory. If you do so, the editing process of the configuration file will still be incomplete, so save the file after you finish making changes.

2. After editing the running configuration, if you execute the `exit` command without saving the changes to internal flash memory, the startup configuration file in internal flash memory and the running configuration will not be the same. After editing the configuration, you must always save your changes.

```
exit
```

Related commands

None

save (write)

Saves the edited configuration to the startup configuration file.

Syntax

save

write

Parameters

None

Response messages

None

Notes

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

Related commands

None

show

Displays the configuration being edited.

Syntax

show [*<Command>* [*<Parameter>*]]

Parameters

<Command>

Specifies a configuration command.

<Parameter>

Use this parameter to limit the number of items to be displayed.

Notes

1. If there are many items in the configuration, the command might take time to execute.
2. In global configuration mode, *<Command>* `[`*<Parameter>*`]` can be specified for a command that switches to level-2 configuration mode. The command line completion, Help, and abbreviated-command execution functionality can also be used.
3. In level-2 configuration mode, *<Command>* `[`*<Parameter>*`]` can be specified for a command that switches modes, as in global configuration mode. In this case, however, the command line completion functionality and Help functionality cannot be used.

Related commands

None

top

After a switch to configuration command mode, entering this command returns you to global configuration mode (level 1).

Syntax

```
top
```

Parameters

None

Notes

None

Related commands

None

top

4. Login Security and RADIUS

aaa group server radius
aaa authentication login
aaa authentication login end-by-reject
ip access-group
ipv6 access-class
radius-server attribute station-id capitalize
radius-server dead-interval
radius-server host
radius-server key
radius-server retransmit
radius-server timeout
server

aaa group server radius

Configures a RADIUS server group. Entering this command switches to config-group mode in which the RADIUS server group information can be set.

Syntax

To set or change information:

aaa group server radius *<Group name>*

To delete information:

no aaa group server radius *<Group name>*

Input mode

`(config)`

Parameters

<Group name>

Configures the RADIUS server group name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

   We recommend that you use an upper-case letter for the first character.

   However, you cannot use the following character strings:

   - `radius` or a character string beginning with `radius`
   - `tacacs+` or a character string beginning with `tacacs+`

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 valid RADIUS server is not set for the RADIUS server group, the server will not operate.
2. A maximum of four RAIDUS server groups can be set.

Related commands

aaa authentication

dot1x authentication

mac-authentication authentication

web-authentication authentication

web-authentication user-group

aaa authentication login

Specifies the authentication method to be used at remote 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>*]

To delete information:

no aaa authentication login

Input mode

`(config)`

Parameters

default *<Method>* [*<Method>*]

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

group radius

RADIUS authentication is used.

General-use RADIUS servers are used.

local

Local password authentication is used.

group *<Group name>*

RADIUS authentication is used.

The RADIUS server to use is a RADIUS server group. Specify the group name set by the `aaa group server radius` command.

However, you cannot use the following character strings:

- `radius` or a character string beginning with `radius`
- `tacacs+` or a character string beginning with `tacacs+`

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. If `group radius` or `group` *<Group-name>* is specified for the authentication method, communication failure with the RADIUS server or authentication failure at the RADIUS server disables login to the Switch. Therefore, we recommend that you specify local password authentication at the same time.

2. You cannot simultaneously specify both `group radius` (general-use RADIUS server authentication) and `group` *<Group name>* (RADIUS server group authentication), because both methods are treated as RADIUS authentication service. Use either of them in combination with local password authentication.

Related commands

radius-server

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 communication not being possible, such as unresponsive RADIUS server, 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 is denied, 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

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 or FTP).

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 or change information:

ip access-group *<access list name>* in

To delete information:

no ip access-group *<access list name>*

Input mode

`(config-line)`

Parameters

<access list name>

Specifies the ID for an IPv4 filter access list (an ID for `ip access-list standard`).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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 or FTP).
2. To allow FTP connections, set `ftp-server` in config mode.
3. When `ip access-group` is not set, access using IPv4 addresses is permitted from all remote operation terminals.
4. Note that changing the registered IP addresses does not close the sessions of users who have already logged in. The change is applied to users who will log in after this setting.

Related commands

ip access-list standard

line vty

ip access-group

ftp-server

transport input

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 or FTP).

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>* in

To delete information:

no ipv6 access-class *<access list name>*

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 an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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 or FTP).
2. To allow FTP connections, set `ftp-server` in config mode.
3. When `ipv6 access-class` is not set, access using IPv6 addresses is permitted from all remote operation terminals.
4. Note that changing the registered IP addresses does not close the sessions of users who have already logged in. The change is applied to users who will log in after this setting.

Related commands

line vty

ftp-server

ipv6 access-class

transport input

ipv6 access-list

radius-server attribute station-id capitalize

Sends the MAC address that is used for sending data to a RADIUS server with the RADIUS attribute in upper case. The applicable RADIUS attribute names are as follows:

- Called-Station-Id
- Calling-Station-Id

Syntax

To set information:

```
radius-server attribute station-id capitalize
```

To delete information:

```
no radius-server attribute station-id capitalize
```

Input mode

`(config)`

Parameters

None

Default behavior

Sends the MAC address with the RADIUS attribute set in lowercase.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The configuration in this command is applied to authentication requests and accounting requests.
2. The configuration in this command is common to all authentication types (IEEE 802.1X, Web authentication, and MAC-based authentication).
3. The MAC address with the `User-Name` and `User-Password` RADIUS attributes set that is used for MAC-based authentication follows the `mac-authentication id-format` command usage.

Related commands

None

radius-server dead-interval

Configures a monitoring timer that operates for automatically restoring the primary general-use RADIUS server as the current general-use RADIUS server.

The primary general-use RADIUS server is restored when either of the following occurs: The currently operating server (the destination for RADIUS authentication requests) switches to being a valid secondary general-use RADIUS server, or when all servers are disabled, the monitoring timer starts and the period of time set by this command elapses (the monitoring timer expires).

Syntax

To set or change information:

```
radius-server dead-interval <Minutes>
```

To delete information:

```
no radius-server dead-interval
```

Input mode

`(config)`

Parameters

<Minutes>

Specifies the monitoring timer value for automatic restoration of operation to the primary general-use RADIUS server from the secondary general-use RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 1440 (minutes)

   If 0 is set, RADIUS authentication requests are always initiated on the primary general-use RADIUS server.

Default behavior

The primary general-use RADIUS server is automatically restored 10 minutes after the currently operating server switches to the secondary general-use RADIUS server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

1. If the monitoring timer value is changed when the secondary general-use RADIUS server is operating as the current server, the progress to that time is used for judgment purposes and the results are applied.
2. If this command configuration is deleted after the monitoring timer starts, the monitoring timer counter continues without being reset and runs for 10 minutes (default value).

Notes

1. If more than three general-use RADIUS servers are configured and another

general-use RADIUS server becomes the current server after the monitoring timer starts, the monitoring timer is not reset and continues to run.

2. In general, when the monitoring timer has started, it does not reset until it expires. However, as exceptions, it resets in the following cases:
   - When `radius-server dead-interval` 0 is configured by using this command.
   - When information about the general-use RADIUS server running as the current server is deleted by using the `radius-server host` command
   - When the `clear radius-server` operation command is executed
3. If the monitoring timer expires while the authentication sequence is being executed on the terminal subject to authentication, restoration of the primary general-use RADIUS server is not performed until the executed authentication sequence has been completed.

Related commands

aaa authentication

radius-server host

radius-server key

radius-server retransmit

radius-server timeout

radius-server host

Configures the general-use RADIUS server used for authentication.

Syntax

To set or change information:

radius-server host {*<ipv4 address>* | *<ipv6 address>*} [auth-port *<port>*] [acct-port *<port>*] [timeout *<seconds>*] [retransmit *<retries>*] [key *<string>*]

To delete information:

no radius-server host {*<ipv4 address>* | *<ipv6 address>*}

Input mode

`(config)`

Parameters

{*<ipv4 address>* | *<ipv6 address>*}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 address of the RADIUS server in colon notation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <ipv4 address>: IPv4 unicast address

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   <ipv6 address>: IPv6 global unicast address

   ::2 to fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff, fec0:: to feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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:

   Specify a character string that is no more than 64 characters. For details about the characters that can be specified, see *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

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 value is set, the initial value is 3.

2. Range of values:

   0 to 15 (times)

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 (seconds)

Default behavior

Because the RADIUS server is not configured, no RADIUS communication is performed even if `group radius` is specified for `aaa`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of 20 general-use RADIUS servers can be specified per device.
2. `127.*.*.*` cannot be set as an IPv4 address.
3. If the `key` parameter is omitted and the `radius-server key` command is not set, the RADIUS server is disabled.
4. If multiple general-use RADIUS servers are configured, the address displayed first by using the `show radius-server` operation command is the address of the primary general-use RADIUS server. The primary general-use RADIUS server is used as the initial current server (the destination for RADIUS authentication requests during operation).

   If a failure occurs on the primary general-use RADIUS server, the current server becomes the next valid general-use RADIUS server (the secondary general-use RADIUS server). For details about automatic restoration of the primary general-use RADIUS server, see the description about the `radius-server dead-interval` command.

5. If a RADIUS server with the matching IP address has already been registered in the general-use RADIUS server configuration, authentication-specific RADIUS server configuration, or the RADIUS server group configuration, all of these parameters are replaced by the new commands that were entered automatically.

Related commands

aaa authentication

radius-server dead-interval

radius-server key

radius-server retransmit

radius-server timeout

radius-server key

Configures the default RADIUS server key used for authentication on a general-use RADIUS server or an authentication-specific RADIUS server.

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 RADIUS 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:

   Specify a character string that is no more than 64 characters. For details about the characters that can be specified, 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 `key` settings for the `radius-server host`, `dot1x radius-server host`, `mac-authentication radius-server host`, and `web-authentication radius-server host` commands have priority over the setting for this command.

Related commands

aaa authentication

dot1x radius-server host

mac-authentication radius-server host

radius-server host

radius-server retransmit

radius-server timeout

web-authentication radius-server host

radius-server retransmit

Configures the default number of times an authentication request is resent to the general-use RADIUS server used for authentication or to an authentication-specific RADIUS server.

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 (times)

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` settings for the `radius-server host`, `dot1x radius-server host`, `mac-authentication radius-server host`, and `web-authentication radius-server host` commands have priority over the setting for this command.

Related commands

aaa authentication

dot1x radius-server host

mac-authentication radius-server host

radius-server host

radius-server key

radius-server timeout

web-authentication radius-server host

radius-server timeout

Configures the default response timeout value for the general-use RADIUS server used for authentication or for an authentication-specific RADIS server.

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 (seconds)

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` settings for the `radius-server host`, `dot1x radius-server host`, `mac-authentication radius-server host`, and `web-authentication radius-server host` commands have priority over the setting for this command.

Related commands

aaa authentication

dot1x radius-server host

mac-authentication radius-server host

radius-server host

radius-serve key

radius-server retransmit

web-authentication radius-server host

server

Configures a RADIUS server host in the RADIUS server group.

Syntax

To set or change information:

server {*<ipv4 address>* | *<ipv6 address>*} [auth-port *<port>*] [acct-port *<port>*]

To delete information:

no server {*<ipv4 address>* | *<ipv6 address>*}

Input mode

```
(config-group)
```

Parameters

{*<ipv4 address>* | *<ipv6 address>*}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 address of the RADIUS server in colon notation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <ipv4 address>: IPv4 unicast address

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   <ipv6 address>: IPv6 global unicast address

   ::2 to fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff, fec0:: to feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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

Default behavior

Because no RADIUS server is set, no communication is performed by the RADIUS server group.

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 for each group.
2. `127.*.*.*` cannot be set as an IPv4 address.
3. The configuration of this command must meet both of the following conditions:
   - The value in this command is the same as the value in the `radius-server host` command (the values of `auth-port` and `acct-port` are also the same).
   - The `radius-server host` command configuration is enabled (the key parameter has been set or the `radius-server key` command has been configured).
4. If multiple RADIUS servers are configured in the same RADIUS server group, the address displayed by using the `show radius-server` operation command is the primary RADIUS server in the RADIUS server group. This primary RADIUS server is used as the first current server (the destination for RADIUS authentication requests). The current server becomes the next RADIUS server in the primary RADIUS server group.

   Note that automatic restoration of the primary RADIUS server is governed by the configuration of the `radius-server dead-interval` command.

Related commands

aaa group server radius

dot1x authentication

mac-authentication authentication

radius-server host

web-authentication authentication

web-authentication user-group

5. Time Settings and NTP

clock timezone
ntp broadcast client
ntp interval
ntp server

clock timezone

Sets the time zone.

The Switch maintains the date and time internally in Coordinated Universal Time (UTC). This clock timezone 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>

Sets 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

   (It is possible to enter other characters, but use only the characters mentioned above.)

<Hours offset>

Sets an offset in hours from UTC in decimal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   -12 to -1, 0, 1 to 12

<Minutes offset>

Sets an offset in minutes from UTC.

1. Default value when this parameter is omitted:

   0

2. Range of values:

   0 to 59 in decimal

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

If you change the Switch's time zone, statistics on CPU usage collected by the Switch will be cleared to zero.

Related commands

set clock

ntp broadcast client

Sets acceptance of time information broadcast from an NTP server.

Syntax

To set information:

ntp broadcast client

To delete information:

no ntp broadcast client

Input mode

`(config)`

Parameters

None

Default behavior

The time information broadcast from the NTP server is not accepted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

If `ntp server` and `ntp broadcast client` are both set, the `ntp server` setting is effective.

Related commands

ntp server

ntp interval

Sets the interval for regularly obtaining time information from an NTP server.

Syntax

To set or change information:

ntp interval *<Interval>*

To delete information:

no ntp interval

Input mode

`(config)`

Parameters

<Interval>

Sets the interval for obtaining time information from the NTP server. The interval is set in seconds in decimal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   120 to 604800 (seconds)

Default behavior

3600 seconds is set as the interval for obtaining time information from the NTP server.

Impact on communication

None

When the change is applied

When the `ntp server` command has been set, the change takes effect immediately after the setting value is changed.

Notes

The setting takes effect if the `ntp server` command has been set.

Related commands

ntp server

ntp server

Sets the address of the NTP server from which time information can be obtained. A maximum of two entries can be set.

The addess that is set first is called primary, and the address that is set later is called secondary. If a request to acquire the time from the primary NTP server address fails, a request to acquire time information is sent to the secondary NTP server address.

Syntax

To set or change information:

ntp server *<IP address>*

To delete information:

no ntp server *<IP address>*

Input mode

`(config)`

Parameters

<IP address>

Sets the IPv4 address of the NTP server from which the time information can be obtained.

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

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 `ntp server` and `ntp broadcast client` are both set, the `ntp server` setting is effective.
2. `127.*.*.*` cannot be set as an IPv4 address.

Related commands

ntp interval

6. Host Names and DNS

ip domain lookup
ip domain name
ip domain reverse-lookup
ip host
ip name-server
ipv6 host

ip domain lookup

Disables the the DNS resolver functionality by using the `no ip domain lookup` command.

Syntax

To set information:

no ip domain lookup

To delete information:

ip domain lookup

Input mode

`(config)`

Parameters

None

Default behavior

The DNS resolver functionality is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, the change is not always applied correctly to the currently executing commands (such as the `traceroute` operation command).

Notes

None

Related commands

ip name-server

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:

   1 to 255 characters can be specified. For details about the characters that can be specified, see *Host name* 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. However, the change is not always applied correctly to the currently executing commands.

Notes

None

Related commands

ip name-server

ip domain lookup

ip domain reverse-lookup

Disables the reverse lookup functionality (functionality for using an IP address to search for a host name) of the DNS resolver functionality by using the `no ip domain reverse-lookup` command.

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 functionality is enabled, the reverse lookup functionality is also enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, the change is not always applied correctly to the currently executing commands (such as the `traceroute` operation command).

Notes

1. If the DNS resolver functionality is disabled, it does not operate regardless of this setting.

Related commands

ip domain lookup

ip name-server

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:

   1 to 63 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

<ip address>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies the IPv4 unicast 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. `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 `ip host` command and the `ipv6 host` command, the `ip host` command takes priority, unless IPv6 is explicitly specified (such as the `ping ipv6` operation command).

Related commands

None

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 functionality 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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies the IPv4 unicast address.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, the change is not always applied correctly to the currently executing commands (such as the `traceroute` operation command).

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 to display the execution result of the `traceroute` command).

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

Related commands

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:

   1 to 63 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

<ipv6 address>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies the IPv6 global unicast 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. `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 `ip host` command and the `ipv6 host` command, the `ip host` command takes priority, unless IPv6 is explicitly specified (such as the `ping ipv6` operation command).

Related commands

None

7. Device Management

system fan mode

Sets the operating mode of the Switch fan.

Syntax

To set 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: Cooling-critical setting

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 and 2

Default behavior

Operating mode 1 (Low-noise setting) is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Operation when this command is set differs depending on the Switch model.

Table 7-1 Operation when system fan mode 2 (cooling-critical setting) is set

Model	Fan operation type	Behavior when the command is set
AX2530S-24T AX2530S-24TD	Fanless	Because these models do not have fans, this command is invalid even if it is used.
AX2530S-48T AX2530S-48TD	Semi-fanless	When the cooling-critical setting is selected, the `system fan-control` command setting is invalid (fixed fan speed).
AX2530S-24T4X AX2530S-48T2X AX2530S-24S4X	Fixed fan speed	Behavior for the cooling-critical setting is performed if the command is omitted or the low-noise setting is specified.

Model	Fan operation type	Behavior when the command is set
AX2530S-24S4XD		

Related commands

system fan-control

system l2-table mode

Sets the search method for the Layer 2 hardware table.

Syntax

To set or change 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. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 5

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

Default behavior

`1` is set as the method for searching the table.

Impact on communication

Because the Switch has to be restarted, communication via the Switch stops until the restart process is complete.

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.

Note that if the form of the command changes to `no system l2-table mode` and the Switch is restarted, the operational table search becomes 1.

Notes

1. When this command is entered, the message below appears. Save the configuration and restart the Switch before entering another configuration command.

```
Please execute the reload command after save,
because this command becomes effective after reboot.
```

Related commands

None

system memory-soft-error

Configures the Switch to output a log 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 a log 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

A log 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 recovery

When the `no system recovery` form of the command is set and a failure is detected, the Switch is not restarted and remains in the failure state.

For details about the entities subject to failure and restoration, see *11. Device Management* in the *Configuration Guide Vol. 1*.

Syntax

To set information:

no system recovery

To delete information:

system recovery

Input mode

`(config)`

Parameters

None

Default behavior

Restarts the Switch when a failure is detected.

Impact on communication

The link status of all ports is down-link and communication stops.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Automatic restoration stops when system recovery is disabled (`no system-recovery`). If a critical failure (E9 level error) occurs, the Switch is not restarted after the failure log is collected. For details about the automatic restoration disabled status, see *11. Device Management* in the *Configuration Guide Vol. 1*.

Related commands

None

system temperature-warning-level

Outputs a warning message when the intake temperature of the switch 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

<temperature>

Sets the temperature (in Celsius).

The temperature can be set in units of one degree Celsius.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   [24T][24TD]: 25 to 45 (°C)

   Other than above: 25 to 50 (°C)

Default behavior

An operation message is not output when the specified temperature is exceeded.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the following operating environment conditions are not met, the log might be output at a temperature lower than the specified intake temperature:
   - Provide sufficient ventilation to efficiently remove the heat from around the Switches.
   - Do not stack Switches.
   - Do not install Switches vertically.
   - Do not place Switches near heat sources.
2. If the intake temperature of the Switch exceeds the specified temperature, an operation message is immediately output.

Related commands

None

system temperature-warning-level average

Outputs an operation message when the average temperature during the specified period exceeds the specified temperature.

Syntax

To set information:

system temperature-warning-level average [*<temperature>*] [period *<days>*]

To delete information:

no system temperature-warning-level average

Input mode

```
(config)
```

Parameters

<temperature>

Sets the average temperature (in Celsius).

The temperature can be set in units of one degree Celsius.

1. Default value when this parameter is omitted:

   38 (°C)

2. Range of values:

   [24T][24TD]: 25 to 45 (°C)

   Other than above: 25 to 50 (°C)

period *<days>*

Sets the number of days to be used to calculate the average temperature.

1. Default value when this parameter is omitted:

   30

2. Range of values:

   1 to 30

Default behavior

An operation message is not output when the specified average temperature is exceeded.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

The threshold of the average temperature is checked at noon or when the Switch is started.

Notes

1. If the following operating environment conditions are not met, the log might be output at a temperature lower than the specified average temperature:

   - Provide sufficient ventilation to efficiently remove the heat from around the Switches.

- Do not stack Switches.
- Do not install Switches vertically.
- Do not place Switches near heat sources.

2. If the average temperature of the Switch already exceeds the specified value, no operation message is output until the next threshold check is performed.

Related commands

None

```
system temperature-warning-level average
```

8. Power Saving Functionality

power-control port cool-standby
schedule-power-control port cool-standby
schedule-power-control port-led
schedule-power-control shutdown
schedule-power-control system-sleep
schedule-power-control time-range
schedule-power-control wakeup-option
system fan-control
system port-led
system port-led trigger console
system port-led trigger interface
system port-led trigger mc

power-control port cool-standby

Enables power saving operation of the link-down port.

Syntax

To set information:

```
power-control port cool-standby
```

To delete information:

```
no power-control port cool-standby
```

Input mode

`(config)`

Parameters

None

Default behavior

Operation is at normal power consumption.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Because the power saving functionality of link-down ports is not supported for SFP ports and shared SFP/SFP+ ports [10G model], no operation is performed even if this command is set.

Related commands

None

schedule-power-control port cool-standby

Configures power saving operation for link-down ports during scheduled power saving operation.

Syntax

To set information:

```
schedule-power-control port cool-standby
```

To delete information:

```
no schedule-power-control port cool-standby
```

Input mode

`(config)`

Parameters

None

Default behavior

Operation is at normal power consumption when the port is in the link-down state.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Because the power saving functionality of link-down ports is not supported for SFP ports and shared SFP/SFP+ ports [10G model], no operation is performed even if this command is set.

Related commands

None

schedule-power-control port-led

Configures LED operation during scheduled power saving.

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

Turns on the Switch LED according to the operating status.

When the `system port-led trigger` command is not set:

Regardless of the operating status, the LED turns on and blinks with normal brightness.

When the `system port-led trigger` command is set:

Operates under the following conditions:

1. The LED switches to normal brightness when automatic operation is triggered, and then it turns on and blinks.
2. 60 seconds after automatic operation finishes, the LED switches to power saving brightness, and then turns on and blinks.
3. 10 minutes after power saving brightness started, the LED turns off. If any automatic operation is performed during this period, the LED switches to normal brightness, and then turns on and blinks.

economy

Regardless of operation status, the Switch turns on and blinks with power saving brightness.

disable

Regardless of the operating status, the Switch LED turns off.

At this time, the ST1 LED blinks green at long intervals to indicate that the LED is about to turn off.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `enable, economy, disable`

Default behavior

Regardless of operation status, the Switch turns on and blinks with normal brightness.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the LED has been disabled (turned off), ST1, ST2 and ACC (the memory card access LED) turn on with power saving brightness.
2. The PWR LED always on with normal brightness.

Related commands

schedule-power-control time-range

schedule-power-control shutdown

Sets the port that shuts down while the scheduled power saving functionality is used.

Shutting down the port turns off the power, reducing the amount of power consumed.

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 shut down in list format.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set *<interface id list>* and the specifiable values, see *Specifiable values for parameters*.

interface add *<interface id list>*

Adds a port to be shut down 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 set *<interface id list>* and the specifiable values, see *Specifiable values for parameters*.

interface remove *<interface id list>*

Removes a port to be shut down 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 set *<interface id list>* and the specifiable values, see *Specifiable values for parameters*.

Default behavior

The operating status of a port is a state other than shutdown.

For details about port statuses, see the description of the `show port` or `show interfaces` operation 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 be always shut down regardless of a schedule, you must set both the `shutdown` command and this command.

Related commands

schedule-power-control time-range

schedule-power-control system-sleep

Puts a Switch in the sleep state during the scheduled time range.

Putting the Switch in the sleep state reduces the amount of power consumed.

Syntax

To set information:

```
schedule-power-control system-sleep
```

To delete information:

```
no schedule-power-control system-sleep
```

Input mode

`(config)`

Parameters

None

Default behavior

The Switch does not switch to the sleep state.

Impact on communication

All communications stop during the scheduled time range.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The Switch does not switch to the sleep state during operation in configuration command mode.

Related commands

schedule-power-control time-range

schedule-power-control time-range

Specifies the execution time (for specifying a date, a day of the week, or daily) of scheduled power saving functionality.

Syntax

To set or change information:

`schedule-power-control time-range` *<Entry number>* `{date | weekly | everyday | infinity} action { enable | disable }`

- 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>*

- When infinity is specified:

  infinity

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 (for specifying a date, a day of the week, daily, or infinity)

{ date | weekly | everyday | infinity }

Sets 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.

infinity

Specify as infinity.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

date, weekly, everyday, infinity

Parameters for specifying a date

start-time *<YYMMDD> <HHMM>*

Specifies the start date and time.

YY

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

For example, 00 means the year 2000.

MM

Specify the month in the range from 01 to 12.

DD

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

HH

Specify the hour (00 to 23).

MM

Specify 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 is from 0:00 on January 1, 2000, to 23:59 on January 17, 2038.

end-time *<YYMMDD> <HHMM>*

Specifies the end date and time.

YY

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

For example, 00 means the year 2000.

MM

Specify the month in the range from 01 to 12.

DD

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

HH

Specify the hour (00 to 23).

MM

Specify 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 is from 0:00 on January 1, 2000, to 23:59 on January 17, 2038.

Parameters for specifying weekly

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

Specify the hour (00 to 23).

MM

Specify 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

Specify the hour (00 to 23).

MM

Specify 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>*.

Parameters for specifying everyday

start-time *<HHMM>*

Specifies the start time.

HH

Specify the hour (00 to 23).

MM

Specify 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

Specify the hour (00 to 23).

MM

Specify 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 functionality 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 functionality for the time of execution set by using this command. Thereafter, the following configuration command settings are enabled:

- system port-led
- power-control port cool-standby
- shutdown

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   enable, disable

Default behavior

None

Impact on communication

If sleep mode is set, all communications stop when the scheduled time range starts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there is an overlap of time of execution between different `action` parameters, the `action disable` setting has priority.
2. When the `schedule-power-control system-sleep` command has been set, note the following:
   - The Switch does not switch to the sleep state if the scheduled time of execution arrives during operation in configuration command mode. The Switch goes into sleep mode after exiting configuration command mode (after moving to administrator mode).
   - A configuration that is not saved is lost if the Switch switches to the sleep state. As a result, the following messages appear when configuration command mode ends:

     ```
     Unsaved changes would be lost when the machine goes to sleep!
     Do you exit "configure" without save ? (y/n):
     ```

     Press `n` to execute the save command.

     When time is set for executing scheduled power saving, if the configuration command has not ended, the Switch does not switch to the sleep state.
   - If no key input operations are performed for a certain period of time (60 minutes by default), you are automatically logged out. If you are automatically logged out while editing the configuration and the Switch switches to the sleep state, an unsaved configuration will be lost.
   - If the sleep state continues for 20 days, the sleep state is canceled and the Switch is started. Then, it goes into sleep mode again after startup.

Related commands

None

schedule-power-control wakeup-option

Configures the wakeup-option.

This option clears the sleep state when WOL packet reception from the relevant port or link-up of the relevant port is detected.

Syntax

To set information:

schedule-power-control wakeup-option wol interface *<interface id list>*

schedule-power-control wakeup-option linkup interface *<interface id list>* [down-detect *<min>*]

To delete information:

no schedule-power-control wakeup-option wol

no schedule-power-control wakeup-option linkup

Input mode

`(config)`

Parameters

Parameter of the WOL packet reception detection option

interface *<interface id list>*

Sets the port where the WOL packet reception detection option is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   [24T][24TD] 0/23, 0/24, 0/25, 0/26

   [48T][48T2X][48TD] 0/47, 0/48, 0/49, 0/50

   [24T4X][24S4X][24S4XD] 0/23, 0/24

   For AX2530S-24T, AX2530S-48T, AX2530S-48T2X, AX2530S-24TD, and AX2530S-48TD, a maximum of two ports can be set for use simultaneously. The following table shows available combinations. Note that available setting for AX2530S-24T4X, AX2530S-24S4X, and AX2530S-24S4XD is 0/23 or 0/24 only.

   [24T and 24TD]

0/23	0/24	0/25	0/26
Y	Y	--	--
--	--	Y	Y
Y	--	--	Y
--	Y	Y	--

[48T, 48T2X, and 48TD]

0/47	0/48	0/49	0/50
Y	Y	--	--
--	--	Y	Y
Y	--	--	Y
--	Y	Y	--

Legend: Y: Port that can receive WOL packets --: Combination is unavailable

Parameter of the port link-up detection option

interface *<interface id list>*

Sets the port where the port link-up detection option is to be enabled.

If any of the set ports is linked-up, the state does not move to the sleep state even if the scheduled time is reached.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about the specifiable range of values, see *Specifiable values for parameters*.

down-detect *<min>*

Specify the monitoring time by minutes from when link-down is detected at all the ports where link-up detection has been set during a scheduled time range until when the state moves to the sleep state.

After the link-down monitoring starts when link-down is detected in all the specified ports, and then after the specified time has passed, the state moves to the sleep state.

During this operation, if link-up is detected in any of the specified ports, the link-down monitoring timer returns to 0.

1. Default value when this parameter is omitted:

   5 (minutes)

2. Range of values:

   1 to 60 (minutes)

Default behavior

The detection of WOL packet reception or link-up does not clear the sleep state.

Impact on communication

During a scheduled time range, if the state moves to the sleep state, all the communications stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To set the `schedule-power-control wakeup-option` command, set the `schedule-power-control system-sleep` command in advance.

schedule-power-control wakeup-option

Related commands

schedule-power-control system-sleep

schedule-power-control time-range

system fan-control

Enables the cooling fan control functionality, which operates by monitoring the internal temperature.

Syntax

To set information:

system fan-control

To delete information:

no system fan-control

Input mode

`(config)`

Parameters

None

Default behavior

The fan operates continuously.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Note, however, that when the `no system fan-control` command is executed, it might take more than ten seconds for the change to be applied.

Notes

1. This command applies only to the AX2530S-48T and AX2530-48TD models.
2. Even if this command is set, the cooling fan always operates for the first 10 minutes after the Switch starts.
3. Operation when this command is set differs depending on the Switch model.

Table 8-1 Operation when system fan mode 2 (cooling-critical setting) is set

Model	Fan operation type	Behavior when the command is set
AX2530S-24T AX2530S-24TD	Fanless	Because this model does not have fans, the command is invalid even if it is used.
AX2530S-48T AX2530S-48TD	Semi-fanless	When the cooling-critical setting is selected, the `system fan-control` command setting is invalid (fixed fan speed).
AX2530S-24T4X AX2530S-48T2X AX2530S-24S4X AX2530S-24S4XD	Fixed fan speed	Behavior for the cooling-critical setting is performed if the command is omitted or the low-noise setting is specified.

system fan-control

Related commands

system fan mode

system port-led

Configures a Switch's LED operation.

Syntax

To set or change information:

system port-led { enable | economy | disable }

To delete information:

no system port-led

Input mode

`(config)`

Parameters

enable

Turns on the Switch LED according to the operating status.

When the `system port-led trigger` command is not set:

Regardless of the operating status, the LED turns on and blinks with normal brightness.

When the `system port-led trigger` command is set:

Operates under the following conditions:

1. The LED switches to normal brightness when automatic operation is triggered, and then it turns on and blinks.
2. 60 seconds after automatic operation finishes, the LED switches to power saving brightness, and then turns on and blinks.
3. 10 minutes after power saving brightness started, the LED turns off. If any automatic operation is performed during this period, the LED switches to normal brightness, and then turns on and blinks.

economy

Regardless of operation status, the Switch turns on and blinks with power saving brightness.

disable

Regardless of the operating status, the Switch LED turns off.

At this time, the ST1 LED blinks green at long intervals to indicate that the LED is about to turn off.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   enable, economy, disable

Default behavior

Regardless of operation status, the Switch LED turns on and blinks with normal brightness.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the LED has been disabled (turned off), ST1, ST2 and ACC (the memory card access LED) turn on with power saving brightness.
2. The PWR LED always turns on with normal brightness.
3. During scheduled operation of the power saving functionality, the Switch operates according to the configuration of the `schedule-power-control port-led` command.

Related commands

None

system port-led trigger console

Adds login to and logout from a Switch via a console (RS-232C) connection as a trigger for automatic LED operation.

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

Login to and logout from a Switch via a console (RS-232C) connection are not regarded as conditions for automatic operation.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

system port-led

system port-led trigger interface

Adds link-up and link-down of the specified physical port a trigger for automatic LED operation.

Syntax

To set or change information:

system port-led trigger interface *<interface id list>*

To delete information:

no system port-led trigger interface

Input mode

```
(config)
```

Parameters

<interface id list>

Specify the relevant port.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

Link-up and link-down of a physical port are not regarded as conditions for automatic operation.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

system port-led

system port-led trigger mc

Adds insertion and removal of a memory card a trigger for automatic LED operation.

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 are not regarded as conditions for automatic operation.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

system port-led

```
system port-led trigger mc
```

Part 3: Network Interfaces

9. 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)
```

Parameters

<kbit/s>

Assigns the line bandwidth in kbit/s.

This setting is used for the `ifSpeed`/`ifHighSpeed` (SNMP MIB) value of the applicable line, 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 10000000 kbit/s

   Do not specify a value that exceeds the line speed of the applicable line.

Default behavior

The line speed of the applicable line is 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 line. Note that when this command is set, information can be checked by using the `show interfaces` or `ifDescr` (SNMP MIB) operation command.

Syntax

To set or change information:

description *<String>*

To delete information:

no description

Input mode

`(config-if)`

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:

   Specify a character string that is no more than 64 characters. For details about the characters that can be specified, see *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 (gigabitethernet)

Sets the duplex mode of a port for an Ethernet interface that has a maximum line speed of 1000 Mbit/s.

Syntax

To set or change information:

duplex {half | full |auto}

To delete information:

no duplex

Input mode

```
(config-if)
```

Parameters

{half | full |auto}

Sets the connection mode of a port to half duplex (fixed), full-duplex (fixed), or auto-negotiation.

The parameters that can be set are vary depending on the port or line type. The following table shows the combinations of line type/port and parameters that can be set. `auto` is selected if a non-specifiable parameter is specified.

Table 9-1 Parameters that can be set for each port

Model	Port	Parameters that can be set
AX2530S-24T AX2530S-24T4X AX2530S-24S4X AX2530S-24TD AX2530S-24S4XD	0/1 to 0/24	half, full, auto
	0/25 to 0/28	full, auto
AX2530S-48T AX2530S-48T2X AX2530S-48TD	0/1 to 0/48	half, full, auto
	0/49 to 0/52	full, auto

Table 9-2 Parameters that can be set for each line type

Line type	Parameters that can be set
10BASE-T/100BASE-TX/1000BASE-T	half, full, auto
100BASE-FX [24S4X][24S4XD]	full
1000BASE-X	full, auto

half

Sets the port to half duplex (fixed) mode.

full

Sets the port 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:

   half, full, auto

Default behavior

`auto` is set.

Impact on communication

If this command is set for the port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

Also, a line test is aborted while it is being performed.

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 set for `speed` or `duplex`, auto-negotiation is performed.
2. For 1000BASE-X, if you do not want to use auto-negotiation, set `1000` for `speed` and `full` for `duplex`. If `auto` or `auto 1000` is set for speed, `full` is set for `duplex` as a result of the auto-negotiation.
3. If the RJ45 port is used with fixed settings, MDI-X is selected.
4. For 100BASE-FX, set `full` for `duplex`. [24S4X][24S4XD]
5. The `half` parameter setting has an effect only for 10BASE-T/100BASE-TX.

Related commands

speed (gigabitethernet)

duplex (tengigabitethernet) [10G model]

Sets the duplex mode of the shared SFP/SFP+ port for 1000BASE-X.

Syntax

To set or change information:

duplex { auto | full }

To delete information:

no duplex

Input mode

`(config-if)`

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:

   auto, full

Default behavior

`auto` is set.

Impact on communication

If this command is set for the port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

Also, a line test is aborted while it is being performed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For 10GBASE-R, the setting for `duplex` and `speed` are disabled.
2. For 1000BASE-X, if auto-negotiation is not used, you must set `speed` to `1000` and `duplex` to `full`.

Related commands

speed (tengigabitethernet)

flowcontrol

Sets flow control.

Syntax

To set or change information:

flowcontrol send {desired | on | off}

flowcontrol receive {desired | on | off}

To delete information:

no flowcontrol send

no flowcontrol receive

Input mode

```
(config-if)
```

Parameters

send {desired | on | off}

Sets send operation for the pause packets of the flow control functionality. Specify the same settings as those for the receive operation for the pause packets of the flow control functionality at the destination.

desired

If fixed mode is set, pause packets are sent. If the auto-negotiation functionality is set, whether pause packets are sent is determined through communication with the connected Switch.

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:

   send desired, send on, send off

receive {desired | on | off}

Sets receive operation for the pause packets of the flow control functionality. Specify the same settings as those for the send operation for the pause packets of the flow control functionality at the destination.

desired

Pause packets are received. If the auto-negotiation functionality is set, whether pause packets are received is determined through communication with the connected Switch.

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:

   receive desired, receive on, receive off

Default behavior

Behavior varies depending on the port or line type.

- gigabitethernet port
  - For 10BASE-T, 100BASE-TX, or 1000BASE-T:

    Receive operation is `off` but send operation is `desired`.
  - For 1000BASE-X:

    Receive operation is `off` but send operation is `desired`.
  - For 100BASE-FX [24S4X][24S4XD]

    Receive operation is `off` but send operation is `on`.
- tengigabitethernet port [10G model]
  - For 1000BASE-T:

    Receive operation is `desired` but send operation is `off.`
  - For 1000BASE-X:

    Receive operation is `desired` but send operation is `off.`
  - For 10GBASE-R:

    Receive operation is `on` but send operation is `off`.

Impact on communication

If this command is set for the port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

Also, a line test is aborted while it is being performed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `desired` is set and auto-negotiation is set, operation is determined based on negotiation. For any setting other than auto-negotiation, `flowcontrol` is fixed to `on`.
2. For 100BASE-FX, no specific operation is performed when auto-negotiation is set because auto-negotiation is not supported. [24S4X][24S4XD]
3. For 10GBASE-R, no specific operation is performed when auto-negotiation is set because auto-negotiation is not supported. [10G model]

Related commands

None

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.

Syntax

To set or change information:

interface gigabitethernet *<IF#>*

Input mode

`(config)`

Parameters

<IF# >

Sets the interface 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

1. The port name is `geth` + *interface-port-number*.

   Example: The name of the 0/1 port will be `geth0/1`.

2. This command cannot be deleted.

Related commands

None

interface tengigabitethernet [10G model]

Sets the 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.

Syntax

To set or change information:

interface tengigabitethernet *<IF#>*

Input mode

`(config)`

Parameters

<IF# >

Sets the interface 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

1. The port name is `tengeth` + *interface-port-number*.

   Example: The name of the 0/25 port will be `tengeth0/25`.
2. This command cannot be deleted.

Related commands

None

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 for this command, temporary link-downs will not be detected so the link will be prevented from becoming unstable.

Syntax

To set or change information:

link debounce [time *<milli seconds>*]

To delete information:

no link debounce

Input mode

```
(config-if)
```

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 in milliseconds

Default behavior

2000 milliseconds is set.

Impact on communication

A line test is aborted while it is being performed.

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, or 1000BASE-T, 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)
```

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 operating value is 1000 milliseconds. When the line speed is set to auto-negotiation, the operating value is 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 fault 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 MDI functionality of the port to be used. When `no mdix auto` is specified, the automatic MDIX functionality 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)`

Parameters

None

Default behavior

During auto-negotiation, MDI and MDI-X are switched automatically.

Impact on communication

If this command is set for the port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

Also, a line test is aborted while it is being performed.

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. This command cannot be specified for the SFP port. (Except for the SFP-T)
3. For 1000BASE-X, this command is disabled.
4. For 100BASE-FX, this command is disabled. [24S4X][24S4XD]:
5. For 10GBASE-R, this command is disabled. [10G model]

Related commands

None

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)`

Parameters

<Length>

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 about the frame format, see *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.

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 9-3 Initial values for the MTU of ports

Presence of the system mtu command	Initial value
Set	Setting value for `system mtu`
Not set	1500

Impact on communication

A line test is aborted while it is being performed.

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 frame length that can be sent or received (the maximum length of frames in Ethernet V2 format#, excluding the FCS).

   #: For details about the frame format, see *14.1.3 Control on the MAC and LLC* *sublayers* in the *Configuration Guide Vol. 1*.

Table 9-4 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 (full and half-duplex), 100BASE-TX (half-duplex)	Not related	Not related	Tagged 1518 Untagged 1514	1500
Others	Set	Not related	Tagged M1[#1]+18 Untagged M1[#1]+14	M1[#1]
	Not set	Set	Tagged M2[#2]+18 Untagged M2[#2]+14	M2[#2]
		Not set	Tagged 1518 Untagged 1514	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, the following operation is performed:
   - If the MTU of the output port is smaller than the MTU of the input port, and the length of the frames to be forwarded exceeds the maximum length of frames that can be sent on the output port, the MTU on the output port is discarded.
3. For two-row 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 tags, set a value larger than 1504 for `mtu`.

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)`

Parameters

None

Default behavior

None

Impact on communication

A line test is aborted while it is being performed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When `Set` of `ifAdminStatus` is executed by the `SetRequest` operation of SNMP from the SNMP manager, the setting is applied to this command.
2. During scheduled operation of power saving functionality, the device operates according to the configuration of the `schedule-power-control shutdown` command.
3. If you want a port to be always shut down regardless of a schedule, you must set both the `schedule-power-control shutdown` command and this command.

Related commands

None

speed (gigabitethernet)

Sets the speed of a port for an Ethernet interface that has a maximum line speed of 1000 Mbit/s.

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)`

Parameters

{ 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 10 100 | 10 100 1000} }

Sets the line speed.

The parameters that can be set are vary depending on the port or line type. The following table shows the combinations of line type/port and parameters that can be set. `auto` is selected if a non-specifiable parameter is specified.

Table 9-5 Parameters that can be set for each port

Model	Port	Parameters that can be set
AX2530S-24T AX2530S-24T4X AX2530S-24S4X AX2530S-24TD AX2530S-24S4XD	0/1 to 0/24	10 100 1000 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
	0/25 to 0/28	1000 auto auto 1000
AX2530S-48T AX2530S-48T2X AX2530S-48TD	0/1 to 0/48	10 100 1000 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
	0/49 to 0/52	1000 auto auto 1000

Table 9-6 Parameters that can be set for each line type

Line type	Parameters that can be set
10BASE-T/ 100BASE-TX/ 1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
100BASE-FX [24S4X][24S4XD]	100
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.

auto

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 cannot be performed at the specified line speed, the status of the link does not switch to the link-up state.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10, 100, 1000, auto, auto {10 | 100 | 1000 | 10 100 | 10 100 1000}

   If `auto` is set, there will be no transition to the link-up state.

Default behavior

`auto` is set.

Impact on communication

If this command is set for the port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

Also, a line test is aborted while it is being performed.

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 set 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` or `half`.
3. For 1000BASE-X, if auto-negotiation is not used, you must set `speed` to `1000` and `duplex` to `full`.
4. If the RJ45 port is used with fixed settings, MDI-X is selected.
5. For 100BASE-FX, set `full` for `duplex`. [24S4X][24S4XD]

Related commands

duplex (gigabitethernet)

speed (tengigabitethernet) [10G model]

Sets the speed of the shared SFP/SFP+ port for 1000BASE-X.

Syntax

To set or change information:

speed { auto | 1000 }

To delete information:

no speed

Input mode

`(config-if)`

Parameters

{ auto | 1000 }

Sets the line speed.

auto

Sets the line speed to auto-negotiation.

1000

Sets the line speed to 1000 Mbit/s.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   auto, 1000

Default behavior

`auto` is set.

Impact on communication

If this command is set for the port in use, the port goes down and communication stops temporarily. Thereafter, the port restarts.

Also, a line test is aborted while it is being performed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For 10GBASE-R, the setting for `duplex` and `speed` are disabled.
2. For 1000BASE-X, if auto-negotiation is not used, you must set `speed` to `1000` and `duplex` to `full`.

Related commands

duplex (tengigabitethernet)

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

<Length>

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 about the frame format, see *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.

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

A line test is aborted while it is being performed.

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 about the frame format, see *14.1.3 Control on the MAC and LLC sublayers* in the *Configuration Guide Vol. 1*.

Table 9-7 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)	Line MTU (in octets)
10BASE-T (full and half-duplex), 100BASE-TX (half-duplex)	Not related	Not related	Tagged 1518 Untagged 1514	1500
Others	Set	Not related	Tagged M1[#1]+18 Untagged M1[#1]+14	M1[#1]
	Not set	Set	Tagged M2[#2]+18 Untagged M2[#2]+14	M2[#2]
		Not set	Tagged 1518 Untagged 1514	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 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 tags, set `system mtu` so that the mtu value is set to a value larger than 1504 or set mtu on the port.

Related commands

None

10. Link Aggregation

channel-group lacp system-priority
channel-group max-active-port
channel-group mode
channel-group periodic-timer
description
interface port-channel
lacp port-priority
lacp system-priority
shutdown

channel-group lacp system-priority

Sets the LACP system priority of a 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)`

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 the operating 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 the LACP system priority is changed, the status of all ports registered for the channel group changes to `Blocking` (communication interrupted).

Related commands

interface port-channel

channel-group max-active-port

Sets the maximum number of ports actually used in a channel group for link aggregation.

Syntax

To set or change information:

channel-group max-active-port *<Number>* [no-link-down]

To delete information:

no channel-group max-active-port

Input mode

`(config-if)`

Parameters

<Number> [no-link-down]

Specifies the maximum number of ports that will be used for link aggregation in a channel group. If the number of ports that can be 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 functionality is applied to the rest of the ports. If you use the standby link functionality in link-not-down mode, set the `no-link-down` command. If you do not do so, the standby link switches to the link-down stats. 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 a port with a larger interface port number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8

Default behavior

The maximum number is 8.

Impact on communication

The ports that are in use might be changed by the standby link functionality, and communication might stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Use this command in static link aggregation mode.
2. If you set 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. To change link-down or no-link-down for the standby link mode, first delete the parameter, and then set it again. To change the number of ports in link-not-down mode, you must set the `no-link-down` command.

channel-group max-active-port

Related commands

interface port-channel

channel-group lacp system-priority

lacp system-priority

lacp port-priority

channel-group mode

Creates a channel group for link aggregation.

Syntax

To set information:

channel-group *<Channel group#>* mode { on | { active | passive } }

To change information:

channel-group *<Channel group#>* mode { active | passive }

To delete information:

no channel-group

Input mode

`(config-if)`

Parameters

<Channel group#>

Sets 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 } }

Sets 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:

   `on`, `active`, or `passive`

Default behavior

None

Impact on communication

If this setting is specified for the operating 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 you set `channel-group mode`, the command automatically generates the `port-channel` setting of the specified channel group. If the `port-channel` setting already exists, the command does not do anything.
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 configuration commands common to 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 *15.2.4 Configuring a port channel interface* in the *Configuration Guide Vol. 1*.
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

interface gigabitethernet

interface tengigabitethernet

channel-group periodic-timer

Sets the LACPDU sending interval.

Syntax

To set or change information:

channel-group periodic-timer { long | short }

To delete information:

no channel-group periodic-timer

Input mode

`(config-if)`

Parameters

{ long | short }

Sets the interval at which the remote device sends LACPDUs to a Switch.

`long`: 30 seconds

`short`: 1 second

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `long` or `short`

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

interface port-channel

channel-group mode

description

Sets supplementary information.

Syntax

To set or change information:

description *<String>*

To delete information:

no description

Input mode

`(config-if)`

Parameters

<String>

Sets supplementary information for the applicable channel group 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:

   Specify a character string that is no more than 64 characters. For details about the characters that can be specified, see *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.

Syntax

To set or change information:

interface port-channel *<Channel group#>*

To delete information:

no interface port-channel *<Channel group#>*

Input mode

`(config)`

Parameters

<Channel group#>

Sets 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*.

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.

Related commands

interface gigabitethernet

interface tengigabitethernet

interface range

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)`

Parameters

<Priority>

Sets the port priority. The lower the value, the higher the priority.

When `on` is set 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 set the port priority for the operating port by setting `channel-group mode` to `active` or `passive`, communication is temporarily interrupted. If you set the port priority for the operating port by setting `channel-group mode` to `on`, the port in use is changed by the standby link functionality, and communication might temporarily stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you set the `max-active-port` command, match its setting to the setting 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

interface gigabitethernet

interface tengigabitethernet

channel-group mode

channel-group max-active-port

lacp system-priority

Sets the LACP system priority for a channel group for which the `channel-group lacp system-priority` command is not set.

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 is not set for the channel group, the LACP system priority is set to 128.

Impact on communication

If a priority is set for the operating 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 the LACP system priority is changed, the status of all ports registered for the channel group changes to `Blocking` (communication interrupted).

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)`

Parameters

None

Default behavior

None

Impact on communication

If the priority is set for an operating channel group, the channel group goes down.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

When `Set` of `ifAdminStatus` is executed by the `SetRequest` operation of SNMP from the SNMP manager, the setting is applied to this command.

Related commands

interface port-channel

shutdown

Part 4: Layer 2 Switching

11. MAC Address Table

mac-address-table aging-time
mac-address-table static

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 set, 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.
2. When any of the following settings is in effect, an aging time of 10 to 300 seconds set by this command is set to 300 seconds.

- `dot1x auto-logout` is valid
- `web-authentication auto-logout` is valid.
- `mac-authentication auto-logout` is valid.

Related commands

None

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 { gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>* }

To delete information:

no mac-address-table static *<MAC>* vlan *<VLAN ID>*

Input mode

`(config)`

Parameters

<MAC>

Sets the 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 lower bit is set to 1) cannot be set.

vlan *<VLAN ID>*

Sets 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 { gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>* }

Sets the output destination interface for static entries. A physical port or link aggregation can be set for the interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <IF#>: See *Specifiable values for parameters*.

   <Channel group#>: See *Specifiable values for parameters*.

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 set, 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 the output destination interface and the VLAN specified by using this command are operating using automatic VLAN assignment of the Layer 2 authentication functionality, the MAC address cannot be registered as a static entry.

Related commands

vlan

12. VLAN

- interface vlan
- l2protocol-tunnel eap
- l2protocol-tunnel stp
- mac-address
- name
- protocol
- state
- switchport access
- switchport dot1q ethertype
- switchport isolation
- switchport mac
- switchport mac auto-vlan
- switchport mode
- switchport protocol
- switchport trunk
- switchport vlan mapping
- switchport vlan mapping enable
- vlan
- vlan-dot1q-ethertype
- vlan-protocol

interface vlan

Configures a VLAN interface. Setting the VLAN interface allows you to set IP addresses for VLANs.

Syntax

To set or change information:

interface vlan *<VLAN ID>*

To delete information:

no interface vlan *<VLAN ID>*

Input mode

`(config)`

Parameters

<VLAN ID>

Sets the 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 that the default VLAN (VLAN ID = 1) cannot be set 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 generated. Generated VLANs are port VLANs. For a protocol VLAN or MAC VLAN, the VLAN must be generated 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>*.

3. Setting `no vlan` for a VLAN generated by the `interface vlan` command deletes the VLAN. Also, setting the `no interface vlan` command for a VLAN generated by the `vlan` command deletes the VLAN.

Related commands

vlan

l2protocol-tunnel eap

Enables the EAPOL forwarding functionality. The functionality is set for a switch.

Syntax

To set information:

```
l2protocol-tunnel eap
```

To delete information:

```
no l2protocol-tunnel eap
```

Input mode

`(config)`

Parameters

None

Default behavior

The EAPOL forwarding functionality is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

l2protocol-tunnel stp

Enables the BPDU forwarding functionality. The functionality is set for a switch.

Syntax

To set information:

```
l2protocol-tunnel stp
```

To delete information:

```
no l2protocol-tunnel stp
```

Input mode

`(config)`

Parameters

None

Default behavior

The BPDU forwarding functionality is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

mac-address

Sets the MAC address used to identify a MAC VLAN.

Syntax

To set or change information:

mac-address *<MAC>*

To delete information:

no mac-address *<MAC>*

Input mode

```
(config-vlan) (MAC VLAN only)
```

Parameters

<MAC>

Sets the MAC address that will be set for the MAC VLAN. The `mac-address` 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

The MAC address is not set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A MAC address that has been assigned to another VLAN cannot be set. Assign the address to a MAC VLAN after deleting its existing configuration.
2. If a MAC address dynamically configured by using the Layer 2 authentication functionality has been set, the Layer 2 authentication settings are disabled, and the `mac-address` settings take effect.
3. The number of MAC addresses that can be set for a Switch is 64.

Related commands

None

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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*. This parameter cannot be specified if *<VLAN ID list>* has been set by using the `vlan` command.

Default behavior

The initial value is `VLAN`*xxxx*. 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

1. Note the following when using a VLAN name configured by using this command as a VLAN after RADIUS authentication:
   - Specify a unique VLAN name. If the same VLAN name is used for two or more VLANs, the smallest VLAN ID is assigned as the post-authentication VLAN in RADIUS authentication mode.
   - Do not specify a number at the beginning of the VLAN name. A number at the beginning will be recognized as the VLAN ID, which might result in an authentication failure.

Related commands

None

protocol

Sets the protocol for identifying VLANs in protocol VLANs.

Syntax

To set or change information:

protocol *<Protocol name>*

To delete information:

no protocol *<Protocol name>*

Input mode

`(config-vlan)`

Parameters

<Protocol name>

Sets the protocol name of a protocol VLAN. The `protocol` command can be set only when the applicable VLAN is a protocol VLAN. If you want to use multiple protocol names for a single VLAN, set the command separately for each protocol name used.

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:

   `suspend` or `active`

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

When `Set` of `ifAdminStatus` is executed by the `SetRequest` operation of SNMP from the SNMP manager, the setting is applied to this command.

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)
```

Parameters

vlan *<VLAN ID>*

Sets the access port VLAN. Specifiable VLANs are port VLANs or MAC VLANs. A protocol VLAN cannot be set. 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 tagged frame of a port VLAN is received, the frame is handled by the port VLAN. If a tagged frame of a VLAN other than a port VLAN is received, the frame is discarded.
2. In VLAN tunneling mode, frames are handled by port VLANs irrespective of whether they are tagged or untagged.

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)`

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 (including `vlan-dot1q-ethertype`) can be specified per Switch.

Related commands

None

switchport isolation

Configures the inter-port relay blocking functionality.

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)`

Parameters

interface *<interface id list>*

Sets a list of physical ports where forwarding is blocked. Forwarding from a port set by this parameter to the applicable port 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 where forwarding is blocked 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 where forwarding is blocked 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 blocked.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The inter-port relay suppression functionality is entered from the port set by `interface` of the `switchport isolation` command, and discards frames output from the port on which the Switch port isolation command is set. To suppress forwarding on both ends, set the command on both ports.

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>* }

switchport mac dot1q vlan{*<VLAN ID list>* | add *<VLAN ID list>* | 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)`

Parameters

vlan *<VLAN ID list>*

Specifies the list of valid MAC VLANs that applies to a switch port. When this parameter is changed, the effective MAC VLAN list is replaced by the list set for the parameter.

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 receives frames that have an unregistered source MAC address. 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. In addition, the tagged frames can be forwarded in the VLAN set by using this parameter. If a tagged frame is received by another VLAN, the frame is discarded.

Specifiable VLANs are port VLANs or MAC VLANs. A VLAN set by using the `switchport mac vlan` command cannot be set.

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. Specifiable VLANs are port VLANs or MAC VLANs. A VLAN set by using the `switchport mac vlan` command cannot be set.

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 port has been set by using the `switchport mode mac` command and the `switchport mac` command has not been set, only the default VLAN operates.

However, a MAC VLAN specified as a post-authentication VLAN by linking with the authentication functionality 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. If a VLAN is automatically assigned by automatic VLAN assignment of the Layer 2 authentication functionality to a MAC port subject to authentication and either of the following occurs, the authentication cannot be canceled:
   - Setting in the applicable VLAN by using `switchport mac vlan` or `switchport mac vlan add`
   - Deletion in the applicable VLAN by using `no switchport mac` or `switchport mac vlan remove`
2. Even if the VLAN specified by the `switchpoint mac dot1q vlan` command has been already specified as the authenticated VLAN of the dynamic VLAN authentication, the applicable dynamic VLAN authentication is not automatically canceled.

Related commands

switchport mode

vlan mac-based

switchport mac auto-vlan

The `no switchport mac auto-vlan` command enables communication only when the VLAN authenticated by the authentication functionality matches the VLAN specified with the `switchport mac vlan` command.

Syntax

To set information:

no switchport mac auto-vlan

To delete information:

switchport mac auto-vlan

Input mode

`(config-if)`

Parameters

None

Default behavior

The VLAN authenticated by the authentication functionality is not checked against the VLAN specified with the `switchport mac vlan` command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Setting this command cancels the dynamic VLAN authentication of the terminal where the VLAN that has not been specified by the `switchport mac vlan` command is specified as the authenticated VLAN.

Related commands

switchport mac vlan

switchport mode

Configures the Layer 2 interface attribute (port type).

Syntax

To set or change information:

switchport mode {access | trunk | protocol-vlan | mac-vlan | dot1q-tunnel }

To delete information:

no switchport mode

Input mode

`(config-if)`

Parameters

{access | trunk | protocol-vlan | mac-vlan | dot1q-tunnel }

Configures the Layer 2 interface attribute (port type).

access

Sets the applicable interface as an access port. When non-VLAN tunneling is used, untagged frames are sent. When VLAN tunneling is used, frames are sent or received regardless that they are Tagged or Untagged. The access port is available only for one VLAN.

trunk

Sets the applicable interface as a trunk port. A trunk port sends and receives untagged frames and tagged frames.

protocol-vlan

Sets the applicable interface as a protocol port. A protocol port sends and receives untagged frames. When a frame is received, the VLAN is determined by the protocol type of the frame. Tagged frames are discarded.

mac-vlan

Sets the applicable interface as a MAC port. A MAC port sends and receives untagged frames. 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 `switchport mac dot1q vlan` command is set, tagged frames are forwarded.

dot1q-tunnel

Sets the applicable interface as a tunneling port. A tunneling port sends and receives untagged frames and tagged frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `access`, `trunk`, `protocol-vlan`, `mac-vlan`, or `dot1q-tunnel`

Default behavior

`access` (access port) is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the applicable interface is set as a trunk port, set `allowed vlan` by using the `switchport trunk` command. If an interface is set as a trunk port and `allowed vlan` is not set, all frames on the applicable interface are discarded.
2. If the applicable interface is set as a protocol port, set the protocol VLAN by using the `switchport protocol` command. If the protocol VLAN is not set, the applicable interface operates as an access port.
3. You cannot make changes using this command if the following commands are set for the applicable interface:
   - dot1x port-control
   - mac-authentication port
   - web-authentication port
4. If the applicable interface is set as a tunneling port, use the `switchport access` command to set VLAN. The tunneling ports are not automatically added to the default VLAN. When the default VLAN is used, use the `switchport access` command to explicitly set the VLAN. If the VLAN is not set, communication is not possible.
5. If there are any tunneling ports are configured on the Switch, the entire switch enters VLAN tunneling mode. As a result, an access ports also operate as the tunneling ports.

Related commands

None

switchport protocol

Sets the protocol 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)`

Parameters

vlan *<VLAN ID list>*

Sets the currently-valid protocol VLANs on the port. When this parameter is changed, the effective protocol VLAN list is replaced by the list set for the parameter.

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 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 port operates as an access port.
2. If multiple protocol VLANs are set for a protocol 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)`

Parameters

native vlan *<VLAN ID>*

Sets the native VLAN (VLAN that sends and receives untagged frames). Specifiable VLANs are port VLANs or MAC 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 set are discarded.

To send and receive untagged frames, you must set 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 VLAN list that is set.

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 VLAN list that is set.

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 trunk port has been set by using the `switchport mode trunk` command and the `switchport trunk` command is omitted, communication is impossible.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

If the applicable interface is set as a trunk port, you must set `allowed vlan`. If you do not set `allowed vlan`, no frames are sent or received through the applicable interface.

If untagged frames will also be sent and received, you must set the same VLAN ID for both of the following parameters:

- allowed vlan
- native vlan

If the ID is not set, the untagged frames on the applicable interface are discarded.

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)`

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 the trunk port.
3. Tag translation does not have an effect on the frames handled by the native VLAN, because frames which are sent or received by it have no tags. 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.

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)`

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 the trunk port.
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

vlan

Sets VLAN-related items.

Syntax

To set or change 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>

Sets the 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 that the default VLAN (VLAN ID = 1) cannot be set when information is deleted.

<VLAN ID list>

Sets multiple VLAN-IDs at one time. If a VLAN ID that is being set for the first time is included, the applicable VLAN is 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 that the default VLAN (VLAN ID = 1) cannot be set when information is deleted.

protocol-based

Set this parameter for protocol VLAN.

1. Default value when this parameter is omitted:

   The VLANs become port VLANs.

2. Note on using this parameter:

   - When configuring protocol VLANs, you must set `protocol-based`.

- Protocol VLANs cannot be assigned to any VLAN established as a port VLAN or a MAC VLAN.
- Protocol VLANs are not available with VLAN tunneling functionality.

mac-based

Set 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 configuring MAC VLANs, you must set `mac-based`.
   - MAC VLANs cannot be specified for any VLANs established as a port VLAN or a protocol VLAN.
   - MAC VLANs are not available with VLAN tunneling functionality.

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 default VLAN are different from those of other normal VLANs.
2. If you set a list by using *<VLAN ID list>*, you can configure multiple VLANs at one time. Note, however, that under some conditions (multi-command mode) lists cannot be set for some commands. For details, see the following table.

No.	Commands:	Available in multi-command mode
1	state {suspend | active}	Y
2	name	N
3	protocol	Y
4	mac-address	N

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.

No.	Parameter	Whether specifiable by the user	Behavior specific to the default VLAN
1	*<VLAN ID>*	F (fixed value)	Set when the Switch is started. Fixed at 1. Cannot be changed or deleted.
2	*<VLAN ID list>*	F (fixed value)	--
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.

No.	Commands:	Parameter	Whether specifiable by the user	Behavior specific to the default VLAN
1	state {suspend | active}	--	Y	--
2	name	*<string>*	Y	--
3	protocol	*<Protocol name>*	N	--
4	mac-address	*<MAC>*	N	--

Legend Y: Can be set; N: Cannot be set; --: Not applicable

5. When the vlan command is used to generate a VLAN, information can be set for the VLAN interface by using the interface vlan command. For VLANs generated by using the vlan command, use the no interface vlan command to delete information. For a VLAN generated by using the interface vlan command, use the no vlan command to delete information.
6. If the automatic assignment of VLANs is specified by using the no vlan command, the VLAN automatically registered on the MAC port is deleted and authentication on the applicable terminal is canceled.

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 Switch.

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-protocol

Sets the protocol name and protocol value for a protocol VLAN.

Syntax

To set or change information:

vlan-protocol *<Protocol name>* [ethertype *<HEX enum>*] [llc *<HEX enum>*] [snap-ethertype *<HEX enum>*]

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:

   Specify a character string that is no more than 14 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

ethertype *<HEX enum>*

Sets 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

llc *<HEX enum>*

Sets the LLC value (DSAP, SSAP) of an 802.3-format frame.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Four-digit hexadecimal

snap-ethertype *<HEX enum>*

Sets 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

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 set by the `protocol` command for the protocol VLAN, the change is applied when the protocol name is set by the `protocol` command.

Notes

1. If a value smaller than 05ff is set for the `ethertype` value (four-digit hexadecimal), 0000 is set.
2. For *<HEX enum>*, one or more `ethertype` values (four-digit hexadecimal) can be set. When you specify multiple values, use a comma (`,`) as the delimiter.
3. `ethertype`, `llc`, and `snap-ethertype` can be entered in any order, but `ethertype`, `llc`, and `snap-ethertype` are displayed in this order for the `show running-config` operation command.
4. A maximum of 16 `ethertype` values can be specified on a single line.
5. The same protocol value cannot be specified multiple times on one line. (Example: `vlan-protocol` *xxx* `ethertype` *<HEX>* `llc`*<HEX>* `ethertype`*<HEX>*).
6. Protocol names set by the `protocol` command cannot be deleted.

Related commands

protocol

13. Spanning Tree Protocols

instance
name
revision
spanning-tree bpdufilter
spanning-tree bpduguard
spanning-tree cost
spanning-tree disable
spanning-tree guard
spanning-tree link-type
spanning-tree loopguard default
spanning-tree mode
spanning-tree mst configuration
spanning-tree mst cost
spanning-tree mst forward-time
spanning-tree mst hello-time
spanning-tree mst max-age
spanning-tree mst max-hops
spanning-tree mst port-priority
spanning-tree mst root priority
spanning-tree mst transmission-limit
spanning-tree pathcost method
spanning-tree port-priority
spanning-tree portfast
spanning-tree portfast bpduguard default
spanning-tree portfast default
spanning-tree single
spanning-tree single cost
spanning-tree single forward-time
spanning-tree single hello-time
spanning-tree single max-age
spanning-tree single mode
spanning-tree single pathcost method
spanning-tree single port-priority
spanning-tree single priority
spanning-tree single transmission-limit
spanning-tree vlan
spanning-tree vlan cost
spanning-tree vlan forward-time
spanning-tree vlan hello-time
spanning-tree vlan max-age
spanning-tree vlan mode
spanning-tree vlan pathcost method
spanning-tree vlan port-priority
spanning-tree vlan priority
spanning-tree vlan transmission-limit

instance

Sets VLANs belonging to Multiple Spanning Tree MST instances.

Syntax

To set or change information:

instance *<MSTI ID>* vlans *<VLAN ID list>*

To delete information:

no instance *<MSTI ID>*

Input mode

`(config-mst)`

Parameters

<MSTI 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 ID list>*

Sets VLANs belonging to MST instances. Either one VLAN ID or multiple VLAN IDs can be set at one time. For a multiple specification, use a hyphen (`-`) or a comma (`,`) to indicate the selection.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

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 `mst` is set for the `spanning-tree mode` command, recalculation of the topology interrupts communication until the topology is formed.

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.

Related commands

spanning-tree mst configuration

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:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *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

`Null` is set for `name`.

Impact on communication

When `mst` is set for the `spanning-tree mode` command, recalculation of the topology interrupts communication until the topology is formed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mst configuration

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 `mst` is set for the `spanning-tree mode` command, recalculation of the topology interrupts communication until the topology is formed.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

spanning-tree mst configuration

spanning-tree bpdufilter

Sets the BPDU filter functionality for the applicable ports. This command is applied to the applicable ports of 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)
```

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 functionality is not valid.

Related commands

None

spanning-tree bpduguard

Sets the BPDU guard functionality for the applicable ports. This command is applied to the applicable ports of PVST+, Single Spanning Tree, and Multiple Spanning Tree, and operates on ports on which the PortFast functionality 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)`

Parameters

{ enable | disable }

Setting `enable` causes the BPDU guard functionality to take effect. Setting `disable` stops operation of the BPDU guard functionality.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `enable` or `disable`

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

None

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 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)`

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.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The value of this command is not applied, if the `spanning-tree vlan cost` command, the `spanning-tree single cost` command, or the `spanning-tree mst cost` command is set.
2. The value of this command is not applied, if the `spanning-tree vlan pathcost method` command or the `spanning-tree single pathcost method` command is set.

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 functionality for 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

None

Related commands

None

spanning-tree guard

Sets the guard functionality for the applicable ports. This command is applied to the applicable ports of 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)`

Parameters

{ loop | none | root }

`loop`: The loop guard functionality is applied to the applicable ports. The loop guard functionality does not operate for Multiple Spanning Tree.

`none`: Stop operation of the loop guard and root guard functionality for the applicable ports.

`root`: The root guard functionality is applied to the applicable ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `loop`, `none`, or `root`

Default behavior

For the loop guard functionality: The setting of the `spanning-tree loopguard default` command is used.

For the root guard functionality: The command does not operate.

Impact on communication

None

When the change is applied

Loop guard setting:

- When the `spanning-tree portfast default` command or the `spanning-tree portfast` command is set, the loop guard setting is not applied.
- If the `spanning-tree portfast default` command and `spanning-tree portfast` command settings have been deleted, loop guard operation starts immediately.

Root guard setting:

- The change takes effect immediately after it is made.

Notes

1. When the `spanning-tree portfast default` command or the `spanning-tree`

`portfast` command is set, the loop guard setting is not applied. Instead, the root guard setting is applied.

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 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)`

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:

   `point-to-point` or `shared`

Default behavior

`point-to-point` is used for a full-duplex port and `shared` is used for a half-duplex port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The automatic restoration functionality is enabled if `point-to-point` is set in STP compatibility mode. The automatic restoration functionality does not operate if `shared` is set in STP compatibility mode.

Related commands

spanning-tree mode

spanning-tree vlan mode

spanning-tree single mode

spanning-tree loopguard default

Sets the loop guard functionality that is used by default. This command is valid for PVST+ and Single Spanning Tree ports.

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 has been set, that setting is used.

If the `spanning-tree guard` command has not been set, the `spanning tree loopguard default` command does not operate.

Impact on communication

None

When the change is applied

- When the `spanning-tree portfast default` command or the `spanning-tree portfast` command is set, the loop guard setting is not applied.
- If the `spanning-tree portfast default` command and `spanning-tree portfast` command settings have been deleted, loop guard operation starts immediately.

Notes

1. When the `spanning-tree portfast default` command or the `spanning-tree portfast` command is set, the loop guard setting is not applied.

Related commands

spanning-tree guard

spanning-tree mode

Sets the operating mode of Spanning Tree Protocols. This command applies to Spanning Tree Protocols (PVST+ and Multiple Spanning Tree) other than Single Spanning Tree. If the `spanning-tree vlan mode` command is set in a PVST+ operating 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 during Spanning Tree operation, 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, Multiple Spanning Tree is applied to all Spanning Tree Protocols. 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:

   `pvst`, `rapid-pvst`, or `mst`

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 *<MSTI ID list>* cost *<Cost>*

To delete information:

no spanning-tree mst *<MSTI ID list>* cost

Input mode

`(config-if)`

Parameters

<MSTI ID list>

Sets an MST instance ID. One MST instance ID can be set. You can use a hyphen (`-`) or a comma (`,`) to set multiple MST instance IDs at one time.

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.

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 cost

spanning-tree mst forward-time

Sets the time required for a Multiple Spanning Tree state 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 state of a port to change.

For ports in stp-compatible mode, only listening and learning states can be maintained for the specified period of time. If a port is not in stp-compatible mode, only discarding and learning states are maintained for the specified period of time (note that this applies only when a timer causes a state transition).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30 (seconds)

Default behavior

The time required for the state 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 interval for sending 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 interval in seconds for sending 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 (seconds)

3. Note on using this parameter:

   If you set 1 then this might result in a changeable topology.

Default behavior

2 seconds is set as the interval for sending BPDUs.

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 (seconds)

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 *<MSTI ID list>* max-hops *<Hop number>*

To delete information:

no spanning-tree mst max-hops

no spanning-tree mst *<MSTI ID list>* max-hops

Input mode

`(config)`

Parameters

<MSTI ID list>

Sets an MST instance ID. One MST instance ID can be set. You can use a hyphen (`-`) or a comma (`,`) to set multiple MST instance IDs at one time.

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 forwarded 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 *<MSTI ID list>* port-priority *<Priority>*

To delete information:

no spanning-tree mst *<MSTI ID list>* port-priority

Input mode

`(config-if)`

Parameters

<MSTI ID list>

Sets an MST instance ID. One MST instance ID can be set. You can use a hyphen (`-`) or a comma (`,`) to set multiple MST instance IDs at one time.

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.

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 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 *<MSTI ID list>* root priority *<Priority>*

To delete information:

no spanning-tree mst *<MSTI ID list>* root priority

Input mode

`(config)`

Parameters

<MSTI ID list>

Sets an MST instance ID. One MST instance ID can be set. You can use a hyphen (`-`) or a comma (`,`) to set multiple MST instance IDs at one time.

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.

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 *<Counts>*

To delete information:

no spanning-tree mst transmission-limit

Input mode

```
(config)
```

Parameters

<Counts>

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 is applied to PVST+ and Single Spanning Tree, but not to Multiple Spanning Tree.

The value of this command is not applied, if the `spanning-tree vlan pathcost method` command or the `spanning-tree single pathcost method` command is set.

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 [10G model]

- 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 [10G model]

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:

   `long` or `short`

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, the Multiple Spanning Tree operates using a 32-bit value. 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 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)`

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.

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 vlan port-priority

spanning-tree single port-priority

spanning-tree mst port-priority

spanning-tree portfast

Sets the PortFast functionality for the applicable ports. This command is applied to the applicable ports of 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)`

Parameters

{ trunk | disable }

If `trunk` is set, the PortFast functionality is applied to access, trunk, protocol, and MAC ports.

If `disable` is set, the PortFast functionality stops.

1. Default value when this parameter is omitted:

   The PortFast functionality, which is enabled on access, protocol, and MAC ports, is applied.

2. Range of values:

   `trunk` or `disable`

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

None

Related commands

spanning-tree portfast default

spanning-tree portfast bpduguard default

Sets the BPDU guard functionality to be used by default. This command is valid for all ports on which the PortFast functionality of PVST+, Single Spanning Tree, and Multiple Spanning Tree 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 operate.

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 portfast default

spanning-tree portfast

spanning-tree bpduguard

spanning-tree portfast default

Sets the PortFast functionality to be used by default. This command is valid on the access, protocol, and MAC ports of 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 default` command does not operate.

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 portfast

spanning-tree single

Starts calculation of the topology for Single Spanning Tree. If the Spanning Tree operating 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 operating mode is Multiple Spanning Tree, Single Spanning Tree does not operate.

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)`

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.

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 cost

spanning-tree pathcost method

spanning-tree single pathcost method

spanning-tree single forward-time

Sets the time required for the state 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 state of a port to change.

If `stp` (802.1D) is set by the `spanning-tree single mode` command, the listening state and the learning state are maintained for the specified period of time. If `rapid-stp` (802.1w) is set by the `spanning-tree single mode` command, the discarding state and the learning state 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 (seconds)

Default behavior

The time required for the state 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 interval for sending 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 interval in seconds for sending 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 (seconds)

3. Note on using this parameter:

   If you set 1 then this might result in a changeable topology.

Default behavior

2 seconds is set as the interval for sending BPDUs.

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 (seconds)

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 operating mode of Single Spanning Tree.

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 during Spanning Tree operation, 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:

   `stp` or `rapid-stp`

Default behavior

`stp` is set for the Single Spanning Tree operating 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 [10G model]

- 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 [10G model]

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:

   `long` or `short`

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)`

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.

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 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.

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 *<Counts>*

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 operates with Single Spanning Tree.

Syntax

To set or change 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 set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

3. Note on using this command:

   If the `spanning-tree single` command has been set, VLAN1 does not operate 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)`

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 set *<VLAN ID list>* and the specifiable 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:

   If `short` is set for the `spanning-tree pathcost method` or the `spanning-tree vlan` *<VLAN ID list>* `pathcost method` command:

   1 to 65535

   If `long` is set for the `spanning-tree pathcost method` or the `spanning-tree vlan` *<VLAN ID list>* `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.

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 cost

spanning-tree pathcost method

spanning-tree vlan pathcost method

spanning-tree vlan forward-time

Sets the time required for PVST+ state 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 set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

<Seconds>

Specifies the time in seconds required for the state of a port to change.

If `pvst` (802.1D) is set for the `spanning-tree mode` command or the `spanning-tree vlan` *<VLAN ID list>* `mode` command, the listening state and the learning state are maintained for the set period of time.

If `rapid-pvst` (802.1w) is set for the `spanning-tree mode` command or the `spanning-tree vlan` *<VLAN ID list>* `mode` command, the discarding state and the learning state 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 (seconds)

Default behavior

The time required for the state 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

spanning-tree vlan forward-time

Related commands

spanning-tree mode

spanning-tree vlan mode

spanning-tree vlan hello-time

Sets the interval for sending 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 set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

<Hello time>

Specifies the interval in seconds for sending 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 (seconds)

3. Note on using this parameter:

   If you set 1 then this might result in a changeable topology.

Default behavior

2 seconds is set as the interval for sending BPDUs.

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 set *<VLAN ID list>* and the specifiable 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 (seconds)

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+ operating 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 set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

{ pvst | rapid-pvst }

Sets the protocol to be used. If the protocol is changed during Spanning Tree operation, 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:

   `pvst` or `rapid-pvst`

Default behavior

The PVST+ operating mode is set by the `spanning-tree mode` command.

Impact on communication

If `pvst` or `rapid-pvst` has been set for the `spanning-tree mode` command, recalculation of the topology interrupts communication until the topology is formed.

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 [10G model]

- 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 [10G model]

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 set *<VLAN ID list>* and the specifiable 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:

   `long` or `short`

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)`

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 set *<VLAN ID list>* and the specifiable 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.

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 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 set *<VLAN ID list>* and the specifiable 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.

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 *<Counts>*

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 set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

<Counts>

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 for the `spanning-tree mode` command or the `spanning-tree vlan` *<VLAN ID list>* `mode` command. When `pvst` (802.1D) is set for the `spanning-tree mode` command or the `spanning-tree vlan` *<VLAN ID list>* `mode` command, the maximum number of BPDUs that can be sent per second is 3 (fixed) and the setting value of this command is not referenced.

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

spanning-tree vlan hello-time

14. Ring Protocol

axrp
axrp virtual-link
axrp vlan-mapping
axrp-primary-port
axrp-ring-port
control-vlan
disable
flush-request-count
flush-request-transmit vlan
forwarding-shift-time
health-check holdtime
health-check interval
mode
multi-fault-detection holdtime
multi-fault-detection interval
multi-fault-detection mode
multi-fault-detection vlan
name
preempt-delay
vlan-group

axrp

Sets the ring ID. In addition, to collect information necessary for the Ring Protocol functionality, switches to config-axrp mode. A maximum of 51 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 switches 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 when the multi-fault monitoring functionality is used, a maximum of 8 ring IDs can be used.

Related commands

None

axrp virtual-link

Sets a virtual link ID used to identify the root bridge shared by a Spanning Tree Protocol. 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 functionality cannot be used concurrently with a Spanning Tree Protocol using a virtual link on the same switch.
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.

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 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 set *<vlan id list>* and the specifiable 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 set *<vlan id list>* and the specifiable values, see *Specifiable values for parameters*.

3. Handling of *<vlan id list>* after a change:

   If the VLAN list is too long after the addition of VLANs, the VLAN list might be divided into multiple lines and the configuration might be displayed as an `axrp vlan-mapping` command that consists of multiple lines. If the VLAN list is shorter after the addition of VLANs, an `axrp vlan-mapping` command that consisted of multiple lines might be consolidated and displayed as the configuration.

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 set *<vlan id list>* and the specifiable values, see *Specifiable values for parameters*.

3. Handling of *<vlan id list>* after a change:

   If the VLAN list is too long after the addition of VLANs, the VLAN list might be divided into multiple lines and the configuration might be displayed as an `axrp vlan-mapping` command that consisted of multiple lines. If the VLAN list is shorter after the removal of VLANs, an `axrp vlan-mapping` command that consisted of multiple lines might be consolidated and displayed as the configuration.

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 to 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 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.
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 operates 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)`

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, no operation is performed.
2. While the Ring Protocol is operating, if you change or delete the primary port, this functionality is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality 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 a 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.

Related commands

mode

axrp-ring-port

axrp-ring-port

Sets an interface that operates 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)`

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 operates 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 operates 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 operates as a standard ring port.

2. Range of values:

   `shared-edge` or `shared`

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 operating 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 functionality is disabled temporarily. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality 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 operates as the primary port.
5. If a shared port is not specified as a shared node, the Ring Protocol functionality will not operate properly.

Related commands

mode

axrp-primary-port

control-vlan

Sets the VLAN to be used as a control VLAN. You can use the VLANs set by using this command to send and receive control frames that monitor the ring status.

Setting `forwarding-delay-time` for a transit node allows you to set the time required to transfer the status of the control VLAN to `Forwarding` during initial operation. 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>

Specifies 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 control VLAN switches to `Forwarding` when a Switch is started in transit node.

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 (seconds)

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 functionality is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality 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 operating mode is transit node.
8. `forwarding-delay-time` operates when the following occurs:
    - The Switch is started (includes execution of the `reload` or `ppupdate` operation command).

Related commands

vlan

disable

Disables the Ring Protocol functionality.

Syntax

To set information:

```
disable
```

To delete information:

```
no disable
```

Input mode

`(config-axrp)`

Parameters

None

Default behavior

The Ring Protocol functionality 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 functionality is disabled. In this case, a loop might occur depending on a network configuration (ring configuration) to which the Ring Protocol functionality 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 (times)

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 neighboring-ring flush control frames to the devices in the neighboring ring configuration to clear the MAC address table when a ring failure occurs or the failure is corrected.

For details about how to specify these settings, see *22.1.11 Configuring flush control frames for neighboring rings* in the manual *Configuration Guide Vol. 1*.

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>

Specify the ID of the VLAN to which neighboring-ring flush control frames 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, neighboring-ring flush control frames 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 functionality 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. Also, make sure this VLAN ID is used for only sending neighboring-ring flush control frames and is not used for forwarding data.

Related commands

vlan

forwarding-shift-time

Sets the reception hold time for flush control frames in transit node.

When the reception hold time passes, if no flush control frames are received, the status of a ring port changes from `Blocking` to `Forwarding`.

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}

Specifies the hold time in seconds until 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.

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

10 seconds is used as the reception hold time for flush control frames.

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 normal status. This could produce a temporary loop.

   Set the hold time value based on the interval at which health-check frames are sent from the master node.

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 link non-monitoring ring shared edge nodes, 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 units of 50 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 (milliseconds)

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 monitoring for recovery 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 interval for sending 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 interval for sending health-check frames in units of 50 milliseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   200 to 60000 (milliseconds)

Default behavior

The interval for sending 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 holdtime` command, a health-check timeout is detected.
2. Set the same interval for sending 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, fault detection will not work properly.
3. If the number of ring IDs is set to 9 or larger, make sure that you set the health-check frame sending interval to at least 1000 milliseconds.

Related commands

None

mode

Sets the operating 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 operating mode.

master

Operates as a master node.

transit

Operates as a transit node.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `master` or `transit`

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

Operates 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>*

Operates 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 Switch.

1. Default value when this parameter is omitted:

   For master nodes, the Switch operates as the master node for a shared link monitoring ring (ring that monitors shared links).

   For transit nodes, the Switch operates as a shared link monitoring ring or a transit node of a shared link non-monitoring ring.

2. Range of values:

   `rift-ring`, `rift-ring-edge1`, or `rift-ring-edge 2`

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 Switch in a ring. If you specify multiple master node Switches, the Ring Protocol functionality will not operate properly.
2. If you change or delete the mode while Ring Protocol is operating, the functionality is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the functionality 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 functionality will not operate properly.

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 units of 50 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 (milliseconds)

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 functionality cannot be used concurrently with a Spanning Tree Protocol using a virtual link on the same switch.
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 interval for sending multi-fault monitoring frames in units of 50 milliseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   500 to 60000 (milliseconds)

Default behavior

The interval for sending multi-fault monitoring frames is 2000 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 functionality cannot be used concurrently with a Spanning Tree Protocol using a virtual link on the same switch.
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 multi-fault monitoring.

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:

   `monitor-enable backup-ring` *<ring id>* or `transport-only`

   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 functionality cannot be used concurrently with a Spanning Tree Protocol using a virtual link on the same switch.

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 monitoring multiple faults.

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 the interface used for failure 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 functionality cannot be used concurrently with a Spanning Tree Protocol using a virtual link on the same switch.
2. You cannot specify a VLAN that is used as a control VLAN by another ring ID.
3. You cannot specify a VLAN that is used as a control VLAN as the multi-fault control VLAN.
4. You cannot specify a VLAN that is used in a VLAN group.

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:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Any 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 delay time between detection of fault recovery by the master node and path switch-back operation.

When this command is set, if the master node detects fault recovery, recovery operations are not performed until the path switch-back 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 switch-back suppression time in seconds.

infinity

The suppression time becomes unlimited and the master node does not start restoration operations until the `clear axrp preempt-delay` operation 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

The path switch-back operation is not suppressed.

Impact on communication

None

When the change is applied

If the ring status is normal, the value is applied to operation immediately after this command is set or changed. If an error occurs in a ring, the value is applied to operation from the next time.

If this command is deleted, the value is applied to operation immediately.

Notes

1. To set this functionality, 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 switch-back operation. If you specify a value smaller than the suppression time for path switch-back operation, a loop might occur.

preempt-delay

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 the ring. In addition, by creating two VLAN groups, loads can be balanced (shared) 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. Either one VLAN mapping ID or multiple VLAN mapping IDs can be set at one time. For a multiple specification, use a hyphen (`-`) or a comma (`,`) to indicate the selection.

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

15. IGMP Snooping

ip igmp snooping (global)

ip igmp snooping (interface)

ip igmp snooping fast-leave

ip igmp snooping mrouter

ip igmp snooping querier

ip igmp snooping (global)

Suppresses the IGMP snooping functionality, when `no ip igmp snooping` is set.

Syntax

To set information:

```
no ip igmp snooping
```

To delete information:

```
ip igmp snooping
```

Input mode

`(config)`

Parameters

None

Default behavior

The IGMP snooping functionality is enabled on a Switch.

Impact on communication

The IGMP snooping functionality stops.

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

None

Related commands

None

ip igmp snooping (interface)

Enables the IGMP snooping functionality on a VLAN interface.

Syntax

To set information:

```
ip igmp snooping
```

To delete information:

```
no ip igmp snooping
```

Input mode

`(config-if)`

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

None

Related commands

None

ip igmp snooping fast-leave

Immediately stops multicast communication to the applicable port if IGMP Leave and IGMPv3 Report (detachment 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)
```

Parameters

None

Default behavior

If IGMP Leave and IGMPv3 Report (detachment 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 (detachment 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 this command is set and IGMP Leave and IGMPv3 Report (detachment request) messages are received. 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

Sets a multicast router port for the VLAN interface.

Syntax

To set or change information:

ip igmp snooping mrouter interface {gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*}

To delete information:

no ip igmp snooping mrouter interface {gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*}

Input mode

`(config-if)`

Parameters

{gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*}

Sets an interface for a multicast router port that has been set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <IF#>: Specify an interface port number belonging to the VLAN.

   <Channel group#>: Specify a channel group number belonging to the VLAN. For details about the specifiable values, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If `ip igmp snooping` is not set for the applicable interface, the IGMP snooping functionality does not operate.
2. To connect a Switch to a multicast router port, enable the IGMP snooping functionality on the destination Switch.
3. If you specify a port number belonging to a port channel for a multicast router port, no operation is performed.

Related commands

ip igmp snooping

ip igmp snooping querier

Enables the IGMP querier functionality on a VLAN interface.

Syntax

To set information:

```
ip igmp snooping querier
```

To delete information:

```
no ip igmp snooping querier
```

Input mode

`(config-if)`

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 set for the applicable interface or the IP address is not set, the querier functionality does not operate.

Related commands

ip igmp snooping

ip address

16. MLD Snooping

ipv6 mld snooping (global)

Suppresses the MLD snooping functionality, when `no ipv6 mld snooping` is set.

Syntax

To set information:

no ipv6 mld snooping

To delete information:

ipv6 mld snooping

Input mode

`(config)`

Parameters

None

Default behavior

Enables the MLD snooping functionality on a Switch.

Impact on communication

The MLD snooping functionality stops.

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

None

Related commands

None

ipv6 mld snooping (interface)

Enables the MLD snooping functionality on a VLAN interface.

Syntax

To set information:

```
ipv6 mld snooping
```

To delete information:

```
no ipv6 mld snooping
```

Input mode

`(config-if)`

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

None

Related commands

None

ipv6 mld snooping source

Sets the source IPv6 address of the MLD snooping functionality to be used on a VLAN interface.

Syntax

To set or change information:

ipv6 mld snooping source *<ipv6 address>*

To delete information:

no ipv6 mld snooping source

Input mode

`(config-if)`

Parameters

<ipv6 address>

Sets the source IPv6 address for the MLD snooping functionality.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The IPv6 link-local address is set in colon notation.

Default behavior

The MLD querier functionality does not operate.

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` or the `ipv6 mld snooping source` command is not set for the applicable interface, the MLD querier functionality does not operate.
2. If multiple interfaces (interface range) are set, the `ipv6 mld snooping source` command cannot be set.
3. Specify the IPv6 link-local address. If the IPv6 global address is specified, a Switch might not operate as a system.
4. The IPv6 address is displayed in abbreviated form.

Related commands

ipv6 mld snooping

ipv6 mld snooping querier

ipv6 mld snooping mrouter

Sets a multicast router port for the VLAN interface.

Syntax

To set or change information:

ipv6 mld snooping mrouter interface {gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*}

To delete information:

no ipv6 mld snooping mrouter interface {gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*}

Input mode

`(config-if)`

Parameters

{gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*}

Sets an interface for a multicast router port that has been set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <IF#>: Specify an interface port number belonging to the VLAN.

   <Channel group#>: Specify a channel group number belonging to the VLAN. For details about the specifiable values, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after the setting value is changed.

Notes

1. If `ipv6 mld snooping` is not set for the applicable interface, this functionality does not operate.
2. To connect a Switch to a multicast router port, enable the MLD snooping functionality on the destination Switch.
3. If you specify a port number belonging to a port channel for a multicast router port, no operation is performed.

Related commands

ipv6 mld snooping

ipv6 mld snooping querier

Enables the MLD querier functionality on a VLAN interface.

Syntax

To set information:

```
ipv6 mld snooping querier
```

To delete information:

```
no ipv6 mld snooping querier
```

Input mode

`(config-if)`

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 set for the applicable interface or the source IPv6 address of the MLD Query message is not set, the MLD querier functionality does not operate.

Related commands

ipv6 mld snooping

ipv6 mld snooping source

Part 5: IP Interface

17. IPv4, ARP, and ICMP

arp

Creates a static ARP table. If a product that does not support ARP is connected, an IPv4 address cannot be converted to a physical address. You need to create a static ARP table in advance.

Syntax

To set or change information:

arp *<ip address>* interface vlan *<vlan id>* *<mac address>*

To delete information:

no arp *<ip address>*

Input mode

`(config)`

Parameters

<ip address>

Specifies a next-hop IPv4 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specifies an IPv4 unicast address.

interface vlan *<vlan id>*

Specifies a VLAN ID.

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.

<mac address>

Specifies the destination MAC address (in a canonical format).

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 lower bit is set to 1) cannot be set.

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

ip address

Sets the local IPv4 address.

Syntax

To set or change information:

ip address *<IP address>* *<Subnet-Mask>* [secondary]

To delete information:

no ip address *<IP address>*

Input mode

```
(config-if)
```

Parameters

<IP address>

Sets the local IPv4 address.

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

<Subnet-Mask>

Sets the subnet mask.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Subnet mask: 128.0.0.0 to 255.255.255.252 (bits must be contiguous)

secondary

Specifies the secondary setting for a multihomed interface.

1. Default value when this parameter is omitted:

   The primary setting is specified. Even if a multihomed interface is used, you need to specify one primary setting.

2. Range of values:

   None

Default behavior

None

Impact on communication

If an interface that is up is changed by using this command, it first goes down and then comes up again.

Accordingly, the following might occur:

- If communication is in progress on the applicable interface, it stops.
- Dynamic ARP entries generated for the applicable interface are deleted.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. `127.*.*.*` cannot be set as an IPv4 address.

Related commands

interface vlan

ip route

Sets a static route IPv4 address.

Syntax

To set or change information:

ip route *<IP address> <Mask> <Next hop>*

To delete information:

no ip route *<IP address> <Mask> <Next hop>*

Input mode

`(config)`

Parameters

<IP address>

Sets the destination IPv4 address for a static route.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0.0.0.0 to 255.255.255.255

<Mask>

Sets the network mask for the destination IPv4 address for the static route.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Subnet mask: 0.0.0.0 to 255.255.255.255 (bits must be contiguous)

<Next hop>

Sets the next hop address on the static route.

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

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

ip mtu

Sets the send IP MTU length for an interface.

Syntax

To set or change information:

ip mtu *<Length>*

To delete information:

no ip mtu

Input mode

`(config-if)`

Parameters

<Length>

Sets the send IP MTU length for an interface. In actuality, the frame length set in port MTU information and this parameter value are compared, and the smaller value is used as the IP MTU length of the interface.

For the frame length set in the port MTU information, see *mtu*.

Use the `show ip interface`, `show ipv6 interface`, or `show ip-dual interface` operation command to check the IP MTU length being used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   128 to 9216 (bytes)

Default behavior

The MTU that has received a router advertisement and the MTU set in the MTU information is compared, and the smaller value is used as the IP MTU length.

If no router advertisement has been received, the frame length (bytes) set in the port MTU information is used as the IP MTU length.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The IP MTU length for Ethernet is set by comparing the frame length set in the port MTU information with the IP MTU value. Therefore, to set a value larger than 1500 for the IP MTU length, check the `ip mtu` settings as well as the `mtu` settings in the port MTU information.

2. To use Web authentication and DHCP server functionality, set the IP MTU length to the default value.

   If the length is shorter than the default, the Web authentication or the DHCP server functionality might not correctly operate.

3. This setting also takes effect for IPv6. For IPv6, the protocol specification defines that the MTU length must be 1280 or larger. Therefore, to use IPv6, do not specify a value smaller than 1280 for the MTU length.
4. If this setting is omitted, the MTU that has received the router advertisement is applied to IPv4.

Related commands

interface vlan

mtu

18. IPv6, NDP, and ICMPv6

ipv6 address

Sets the local IPv6 address.

Syntax

To set or change information:

ipv6 address { *<ipv6 address>*[/*<prefixlen>*] | *<ipv6 prefix>*[/*<prefixlen>*] }

To delete information:

no ipv6 address { *<ipv6 address>*[/*<prefixlen>*] | *<ipv6 prefix>*[/*<prefixlen>*] }

Input mode

`(config-if)`

Parameters

<ipv6 address>

Sets the local IPv6 address.

1. Range of values:

   Specifies an IPv6 global unicast address.

   Note that the address where *<ipv6 address>/<prefixlen>* is `0::/64` or `e80::/10` cannot be specified.

<ipv6 prefix>

Specifies the IPv6 prefix. Specify this parameter to automatically set the interface ID. To set the interface ID automatically, you must set the prefix length to 64.

1. Range of values:

   Specify the IPv6 global unicast address in which the interface ID of the IPv6 address is set to `0`. You cannot specify `0::/64`.

/*<prefixlen>*

Specifies the prefix length.

1. Default value when this parameter is omitted:

   64

2. Range of values:

   1 to 64

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

interface vlan

ipv6 enable

ipv6 default-gateway

Specifies the IPv6 address of the default route.

Syntax

To set information:

For a global address

ipv6 default-gateway *<ipv6 address>*

For a link-local address

ipv6 default-gateway interface vlan *<vlan id>* *<ipv6 address>*

To delete information:

no ipv6 default-gateway

Input mode

`(config)`

Parameters

<ipv6 address>

Specify the IPv6 address of the gateway of the default route.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   When not specifying interface vlan *<vlan id>*

   Specify an IPv6 global unicast address.

   When specifying interface vlan *<vlan id>*

   Specify an IPv6 link local unicast address (`fe80::/64` only).

interface vlan *<vlan id>*

Specifies a VLAN ID.

1. Default value when this parameter is omitted:

   When setting an IPv6 link local unicast address, you cannot omit this parameter.

2. Range of values:

   For *<vlan id>*, specify the VLAN ID set by the `interface vlan` command.

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

interface vlan

ipv6 address

ipv6 enable

ipv6 enable

Specify this command when using IPv6 addresses.

This command automatically generates a link address.

Syntax

To set information:

```
ipv6 enable
```

To delete information:

```
no ipv6 enable
```

Input mode

`(config-if)`

Parameters

None

Default behavior

IPv6 addresses cannot be used.

Specify `ipv6 enable` to use IPv6 addresses.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

interface vlan

ipv6 nd accept-ra

Receives a router advertisement and automatically sets the IPv6 address or the default gateway.

Syntax

To set information:

ipv6 nd accept-ra

To delete information:

no ipv6 nd accept-ra

Input mode

`(config-if)`

Parameters

None

Default behavior

A router advertisement received will be discarded. A router solicitation is not sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Make setting or deletion of this command with the `ipv6 enable` command not set.
2. In the description in *(1) Maximum number of interfaces to which IP addresses can be assigned* and *(2) Maximum number of interfaces where reception can be controlled for each VLAN* in *3.2.4 IP Interfaces* in *Configuration Guide Vol. 1*, an IPv6 address is considered to be set in the VLAN interface with this command set.

Related commands

ipv6 enable

ipv6 neighbor

Creates a static NDP table. If a product that does not support NDP is connected, an IPv6 address cannot be converted to a physical address. You need to create a static NDP table in advance.

Syntax

To set or change information:

ipv6 neighbor *<ipv6 address>* interface vlan *<vlan id>* *<mac address>*

To delete information:

no ipv6 neighbor *<ipv6 address>*

Input mode

`(config)`

Parameters

<ipv6 address>

Specifies a next-hop IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the IPv6 global unicast address (other than `0::/64`) or the IPv6 link local unicast address (`fe80::/64` only).

interface vlan *<vlan id>*

Specifies a VLAN ID.

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.

<mac address>

Specifies the destination MAC address (in a canonical format).

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 lower bit is set to 1) cannot be set.

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 enable

19. DHCP Server Functionality

default-router
dns-server
hardware-address
host
ip dhcp excluded-address
ip dhcp pool
lease
max-lease
network
service dhcp

default-router

Sets the router option that is distributed to clients. A router option is an IP address the client can use as a router IP address over the subnet (default router).

Syntax

To set or change information:

default-router *<IP address>*

To delete information:

no default-router

Input mode

`(dhcp-config)`

Parameters

<IP address>

Sets a router IP address for the subnet of a client (default router).

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

   The following addresses cannot be set:

   - 127.0.0.0 to 127.255.255.255

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of one router IP address (default router) can be set for a pool.

Related commands

ip dhcp pool

dns-server

Sets the domain name server option that is distributed to clients. The domain name server option is the IP address of a DNS server that a client can use.

Syntax

To set or change information:

dns-server *<IP address>* [*<IP address>*]

To delete information:

no dns-server

Input mode

```
(dhcp-config)
```

Parameters

<IP address>

Sets the IP address of the DNS server that a client can use. Specify the address of the server with the highest priority first.

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

   The following addresses cannot be set:

   - 127.0.0.0 to 127.255.255.255

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of two DNS server IP addresses can be specified for a pool.

Related commands

ip dhcp pool

hardware-address

Specifies the MAC address of a client when a static IP address is distributed to the client. This command is used together with the `host` command.

Syntax

To set or change information:

hardware-address *<MAC address> <protocol>*

To delete information:

no hardware-address

Input mode

`(dhcp-config)`

Parameters

<MAC address>

Specifies the MAC addresses corresponding to the DHCP address pool information.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the address in hexadecimal format, separating 2-byte hexadecimal values by periods (.).

   Example: `0211.2233.4455`

<protocol>

Specifies the protocol for the DHCP address pool information. To specify the protocol, you can use a symbol or numeric value.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Only `ethernet` (as a numeric value, only 1)

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 entered together with the `network` command.
2. This command is enabled by setting the `host` command.

Related commands

host

host

Specifies the static IP address to be assigned to a client. This command is used together with the `hardware-address` command.

Syntax

To set or change information:

host *<IP address>* [{ *<Mask>* | /*<Masklen>*}]

To delete information:

no host

Input mode

`(dhcp-config)`

Parameters

<IP address> [{ *<Mask>* | /*<Masklen>*}]

Sets the IP address for the DHCP address pool information. If the mask is omitted, a mask corresponding to class A, B, or C is set.

Table 19-1 IP address range for each class

Class	IP addresses
class A (/8)	`1.`*`x`*`.`*`x`*`.`*`x`* to `126.`*`x`*`.`*`x`*`.`*`x`*
class B (/16)	`128.`*`x`*`.`*`x`*`.`*`x`* to `191.`*`x`*`.`*`x`*`.`*`x`*
class C (/24)	`192.`*`x`*`.`*`x`*`.`*`x`* to `223.`*`x`*`.`*`x`*`.`*`x`*

<IP address>

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The following addresses cannot be set:

   - 127.0.0.0 to 127.255.255.255

   - An address whose host part is all binary 0s or 1s

   - Addresses that do not belong to class A, B, or C

<Mask>

1. Default value when this parameter is omitted:

   A mask corresponding to class A, B, or C

2. Range of values:

   255.0.0.0 to 255.255.255.255

<Masklen>

1. Default value when this parameter is omitted:

   A mask corresponding to class A, B, or C

2. Range of values:

   8 to 32

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 used together with the `network` command in the same pool setting.
2. If there are no `network` or `host` settings for the same subnet when the `host` command is set, that subnet is included in the number of `network` settings. Therefore, for subnets that are beyond the maximum number of managed subnets, a static IP address pool cannot be provided.
3. When the `host` command is set, the optional information (set by the `default-router`, and `dns-server` commands) that will be distributed to clients is inherited from a DHCP address pool. This pool must contain the `network` settings for the same subnet as the specified IP address.
4. This command is enabled by setting the `hardware-address` command.
5. When distributing an IP address to the directly connected subnet (VLAN interface subnet of the Switch), the mask length should be the same as that of the `ip address` command.
6. The mask specified in this command is notified to the client.

Related commands

hardware-address

ip dhcp excluded-address

Sets a range of IP addresses that are to be excluded from distribution in the IP address pool specified by using the `network` command.

Syntax

To set or change information:

ip dhcp excluded-address *<Low address>* [*<High address>*]

To delete information:

no ip dhcp excluded-address *<Low address>* [*<High address>*]

Input mode

`(config)`

Parameters

<Low address> [*<High address>*]

Sets an IP address that cannot be assigned to a DHCP client by a DHCP server or a range of IP addresses.

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

   The following addresses cannot be set:

   - 127.0.0.0 to 127.255.255.255

Default behavior

All IP addresses in the range set by the `network` command can be assigned.

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 IP addresses that can be set is 1024.
2. If the number of IP address pools exceeds the maximum number when the setting for excluded addresses is deleted, you cannot delete the setting.

Related commands

ip dhcp pool

network

ip dhcp pool

Sets DHCP address pool information.

Syntax

To set or change information:

ip dhcp pool *<Pool name>*

To delete information:

no ip dhcp pool *<Pool name>*

Input mode

```
(config)
```

Parameters

<Pool Name>

Specify the name of the DHCP address pool information.

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 14 characters. For details about the characters that can be specified, 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 can set the commands to the sum of the maximum number of managed subnets and the maximum number of static IP addresses.

Related commands

ip dhcp excluded-address

network

lease

Sets the default lease time of the IP addresses distributed to clients.

Syntax

To set or change information:

lease {*<Time day>* [*<Time hour>* [*<Time min>* [*<Time sec>*]]] | infinite}

To delete information:

no lease

Input mode

```
(dhcp-config)
```

Parameters

{*<Time day>* [*<Time hour>* [*<Time min>* [*<Time sec>*]]] | infinite}

Specify the lease time in days, hours, minutes, and seconds. If this information is not set, 1 day is set as the initial value for the lease time. This information cannot be set if the total value of *<Time day> >/<Time hour>/<Time min>/<Time sec>* is less than 10 seconds. Specify a value from 10 (seconds) to 365 (days).

<Time day>

Specify the lease time in days.

1. Range of values:

   0 to 365 (days)

<Time hour>

Specify the lease time in hours.

1. Range of values:

   0 to 23 (hours)

<Time min>

Specify the lease time in minutes.

1. Range of values:

   0 to 59 (minutes)

<Time sec>

Specify the lease time in seconds.

1. Range of values:

   0 to 59 (seconds)

infinite

Sets the lease time to unlimited.

Default behavior

The lease time is set to one day.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a value exceeding the maximum lease time (`max-lease`) is set as the lease time, the maximum lease time has priority.
2. If you set a static IP address, a client has a lease time of 24 hours by default. (However, if a static IP address is distributed to the client, the lease limit is not displayed by the `show ip dhcp binding` command.) In addition, if there is a DHCP address pool that contains the `network` setting for the same subnet as the static IP address, the lease time for that pool has priority.
3. The `lease` command is ignored for a DHCP address pool in which a static IP address has been set.
4. The shorter the lease time set, the more frequently a client updates the lease. Therefore, do not specify an extremely short lease time except for a very limited usage such as a temporary IP address. Also, make sure the client can operate reliably if a short lease time is set.
5. Enter the lease time in the order indicated by the input format. If a value from 24 to 59 is entered after *<Time day>*, the value is treated as *<Time min>*. If you press the **Enter** key in such a case, an input error occurs.

Related commands

ip dhcp pool

max-lease

Sets the maximum allowable lease time when a client specifies the lease time and requests an IP address.

Syntax

To set or change information:

max-lease {*<Time day>* [*<Time hour>* [*<Time min>* [*<Time sec>*]]] | infinite}

To delete information:

no max-lease

Input mode

```
(dhcp-config)
```

Parameters

{*<Time day>* [*<Time hour>* [*<Time min>* [*<Time sec>*]]] | infinite}

Specify the maximum lease time by setting the time in days, hours, minutes, and seconds for the case when the time is specified by the client. If no setting is made for this information, the default lease time is applied. This information cannot be set if the total value of *<Time day>* >/*<Time hour>*/*<Time min>*/*<Time sec>* is less than 10 seconds. Specify a value from 10 (seconds) to 365 (days).

<Time day>

Specify the lease time in days.

1. Range of values:

   0 to 365 (days)

<Time hour>

Specify the lease time in hours.

1. Range of values:

   0 to 23 (hours)

<Time min>

Specify the lease time in minutes.

1. Range of values:

   0 to 59 (minutes)

<Time sec>

Specify the lease time in seconds.

1. Range of values:

   0 to 59 (seconds)

infinite

Sets the lease time to unlimited.

Default behavior

The time set by using the `lease` command is set as the maximum lease time.

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 IP address, a client has a lease time of 24 hours by default. In addition, if there is a DHCP address pool that contains the `network` setting for the same subnet as the static IP address, the maximum lease time for that pool has priority.
2. The `max-lease` command is ignored for a DHCP address pool in which a static IP address has been set.
3. The shorter the lease time set, the more frequently a client updates the lease. Therefore, do not specify an extremely short lease time except for a very limited usage such as a temporary IP address. Also, make sure the client can operate reliably if a short lease time is set.
4. Enter the lease time in the order indicated by the input format. If a value from 24 to 59 is entered after *<Time day>*, the value is treated as *<Time min>*. If you press the **Enter** key in such a case, an input error occurs.

Related commands

ip dhcp pool

network

Sets the subnet of the network in which IP addresses are dynamically distributed via DHCP. Only the subnets whose host bits in the IP address host part are all 0s or 1s are actually registered in the DHCP address pool.

Syntax

To set or change information:

network *<IP address>* [/*<Masklen>*]

To delete information:

no network

Input mode

`(dhcp-config)`

Parameters

<IP address> [/*<Masklen>*]

Sets the network address of the DHCP address pool. If the mask is omitted, a mask corresponding to class A, B, or C is set.

Table 19-2 IP address range for each class

Class	IP addresses
class A (/8)	`1.x.x.x` to `126.x.x.x`
class B (/16)	`128.x.x.x` to `191.x.x.x`
class C (/24)	`192.x.x.x` to `223.x.x.x`

<IP address>

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The following addresses cannot be set:

   - 127.0.0.0 to 127.255.255.255

   - An address whose host part is not 0.

   - IP address that is out of the range shown in Table *19-2 IP address range for each class*.

<Masklen>

1. Default value when this parameter is omitted:

   Mask corresponding to the class A, B, or C shown in *Table 19-2 IP address range for each class*.

2. Range of values:

   8 to 32

   Dot notation (255.0.0.0 to 255.255.255.255) can also be 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. When this command is set, all IP addresses excluding those in which the bits in the host part of the target subnet are all 1s or all 0s are secured as the IP address pool. Therefore, designate IP addresses that should not be distributed in advance by using the `ip dhcp excluded-address` command.
2. This command cannot be set together with the `host` and `hardware-address` commands in the same pool setting.
3. Pools that contain `network` settings can be created up to the maximum number of managed subnets. If there are no `network` or `host` settings that have the same subnet when the `host` command is set, that new subnet is counted towards the maximum number of `network` settings (managed subnets).
4. When distributing an IP address to the directly connected subnet (VLAN interface subnet of the Switch), the mask length should be the same as that of the `ip address` command.

Related commands

ip dhcp excluded-address

ip dhcp pool

service dhcp

Sets the interface on which a DHCP server is enabled. Only the interface specified by using this command receives DHCP packets.

Syntax

To set or change information:

service dhcp vlan *<VLAN ID>*

To delete information:

no service dhcp vlan *<VLAN ID>*

Input mode

`(config)`

Parameters

vlan *<VLAN ID>*

Sets the VLAN ID of a VLAN for which an IPv4 address is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Sets the VLAN ID set by using the `interface vlan` command for *<VLAN 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. A maximum of 64 interfaces can be set.

Related commands

interface vlan

service dhcp

20. Flow Detection Modes

flow detection mode
flow detection out mode

flow detection mode

Sets the flow detection mode for filters and QoS functionality for the receiving-side interface.

This command changes the distribution pattern for the maximum number of entries in a hardware table.

By changing the distribution pattern according to the operating mode, you can collect hardware resource information in the necessary tables and use it.

This command is used to set the basic operating conditions for hardware. If you want to change the distribution pattern, you must delete the `ip access-group`, `ipv6 traffic-filter`, `mac access-group`, `ip qos-flow-group`, `ipv6 qos-flow-group`, and `mac qos-flow-group` commands for the receiving-side interfaces.

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

If you do not set this command or if the information has been deleted, `layer2-2` returns to its default state.

Syntax

To set or change information:

flow detection mode {layer2-1 | layer2-2 | layer2-3}

To delete information:

no flow detection mode

Input mode

`(config)`

Parameters

{layer2-1 | layer2-2 | layer2-3}

Sets the 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 flow detection modes.

Table 20-1 Commands applicable to flow detection mode

Flow detection mode	Applicable command		
	mac	ip	ipv6
	access-group	access-group	traffic-filter
	qos-flow-group	qos-flow-group	qos-flow-group
layer2-1	Y	N	N

Flow detection mode	Applicable command		
	mac	**ip**	**ipv6**
	access-group	**access-group**	**traffic-filter**
	qos-flow-group	**qos-flow-group**	**qos-flow-group**
layer2-2	N	Y	N
layer2-3	N	Y	Y

Legend Y: Can be set; N: Cannot be set

For details about the flow detection modes, see *1.1.3 Receiving-side flow detection mode* in the *Configuration Guide Vol.2* and *3.1.1 Receiving-side flow detection mode* in the *Configuration Guide Vol.2*.

Default behavior

Flow detection operates as Layer 2-2 flow detection.

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

flow detection out mode

Sets the flow detection mode for the filter functionality for the sending-side interface.

This command changes the distribution pattern for the maximum number of entries in a hardware table. By changing the distribution pattern according to the operating mode, you can collect hardware resource information in the necessary tables and use it.

This command is used to set the basic operating conditions for hardware. If you want to change the distribution pattern, you must delete the `ip access-group`, `ipv6 traffic-filter`, and `mac access-group` commands for the sending-side interfaces.

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

If you do not set this command or if the information has been deleted, `layer2-2-out` returns to its default state.

Syntax

To set or change information:

flow detection out mode {layer2-1-out | layer2-2-out | layer2-3-out}

To delete information:

no flow detection out mode

Input mode

`(config)`

Parameters

{layer2-1-out | layer2-2-out | layer2-3-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 20-2 Commands applicable to sending-side flow detection mode

Sending-side flow detection mode	**Applicable command**		
	mac	**ip**	**ipv6**
	access-group	**access-group**	**traffic-filter**
layer-2-1-out	Y	N	N
layer-2-2-out	N	Y	N
layer-2-3-out	Y	Y	Y

Legend Y: Can be set; N: Cannot be set

For details about the sending-side flow detection modes, see *1.1.4 Sending-side flow detection mode* in the *Configuration Guide Vol.2*.

Default behavior

Sending-side flow detection operates as Layer 2-2-out flow detection.

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 detection out mode

Part 7: Filters

21. Access Lists

Names that can be specified

Protocol names (IPv4)

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

Table 21-1 Protocol names that can be specified (IPv4)

Protocol name	Applicable protocol number
ah[#1]	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

#1 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 21-2 Protocol names that can be specified (IPv6)

Protocol name	Applicable protocol number
gre	47
icmp	58
ipv6	All IP protocols
ospf	89

Protocol name	Applicable protocol number
pcp	108
pim	103
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 21-3 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)

Port name	Applicable port name and number
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)
lpd	Printer service (515)
nntp	Network News Transfer Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
pop3s	POP3 over TLS/SSL (995)
raw	Printer PDL Data Stream (9100)
shell	Remote commands (514)
smtp	Simple Mail Transfer Protocol (25)
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 21-4 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)

Port name	Applicable port name and number
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

Table 21-5 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)

Names that can be specified

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

TOS name

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

Table 21-6 TOS names that can be specified

TOS name	TOS value
max-reliability	2
max-throughput	4
min-delay	8
min-monetary-cost	1

TOS name	TOS value
normal	0

Precedence name

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

Table 21-7 Precedence names that can be specified

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

DSCP name

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

Table 21-8 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

Names that can be specified

DSCP name	DSCP value
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 21-9 Ethernet type names that can be specified

Ethernet type name	Ethernet value	Notes
appletalk	0x809b	
arp	0x0806	
eapol	0x888e	
gsrp	--#	Filters GSRP control packets.
ipv4	0x0800	
ipv6	0x86dd	
ipx	0x8137	
xns	0x0600	

#: The value is not made public.

Destination MAC address names

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

Table 21-10 Destination MAC address names that can be specified

Destination address specification	Destination address	Destination address mask
bpdu	0180.C200.0000	0000.0000.0000

Destination address specification	Destination address	Destination address mask
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

Message name (ICMP)

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

Table 21-11 Message names that can be specified for ICMP (IPv4)

Message name	Message	Type	Code
administratively-prohibited	Administratively prohibited	3	13
alternate-address	Alternate address	6	Not specified
conversion-error	Datagram conversion	31	Not specified
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	Not specified
echo-reply	Echo reply	0	Not specified
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1
information-reply	Information replies	16	Not specified

Names that can be specified

Message name	Message	Type	Code
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
time-exceeded	All time exceeded	11	Not specified

Message name	Message	Type	Code
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 21-12 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

Names that can be specified

Message name	Message	Type	Code
parameter-option	Parameter option problems	4	2
parameter-problem	All parameter problems	4	Not specified
port-unreachable	Port unreachable	1	4
reassembly-timeout	Reassembly timeout	3	1
renum-command	Router renumbering command	138	0
renum-result	Router renumbering result	138	1
renum-seq-number	Router renumbering sequence number reset	138	255
router-advertisement	Neighbor discovery router advertisements	134	Not specified
router-renumbering	All router renumbering	138	Not specified
router-solicitation	Neighbor discovery router solicitations	133	Not specified
time-exceeded	All time exceeded	3	Not specified
unreachable	All unreachable	1	Not specified

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, and ICMP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is TCP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is UDP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is ICMP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

To delete information:

no *<seq>*

Input mode

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

Parameters

<seq>

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 | 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:

   - *<protocol>*:

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

     See *Table 21-1 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`.

   - *<source ipv4> <source ipv4 wildcard>* specification:

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

     For *<source ipv4 wildcard>*, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address.

   - `host` *<source ipv4>* specification:

     The filter condition is a perfect match of *<source ipv4>*.

   - `any` specification:

     The source IPv4 address is not included 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 21-3 Port names that can be specified for TCP* and *Table 21-4 Port names that can be specified for UDP (IPv4)*.

   If `eq` is specified, the filter condition is a perfect 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`.

   - *<destination ipv4> <destination ipv4 wildcard>* specification:

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

     For *<destination ipv4 wildcard>*, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address.

   - `host` *<destination ipv4>* specification:

     The filter condition is a perfect match of *<destination ipv4>*.

   - `any` specification:

     The destination IPv4 address is not included 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 21-3 Port names that can be specified for TCP* and *Table 21-4 Port names that can be specified for UDP (IPv4)*.

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

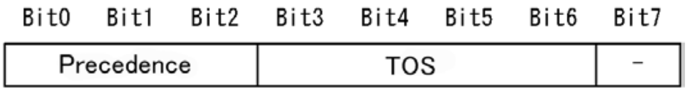
   If `range` is specified, the filter condition is in the range from *<destination port start>* to *<destination port end>*.

   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.



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 21-6 TOS names that can be specified*.

precedence *<precedence>*

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

The value is compared with the first three bits in the TOS field of the received packet.

<table>
<tr><th>Bit0</th><th>Bit1</th><th>Bit2</th><th>Bit3</th><th>Bit4</th><th>Bit5</th><th>Bit6</th><th>Bit7</th></tr>
<tr><td colspan="3">Precedence</td><td colspan="4">TOS</td><td>-</td></tr>
</table>

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 21-7 Precedence names that can be specified*.

dscp *<dscp>*

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

The value is compared with the first six bits in the TOS field of the received packet.

<table>
<tr><th>Bit0</th><th>Bit1</th><th>Bit2</th><th>Bit3</th><th>Bit4</th><th>Bit5</th><th>Bit6</th><th>Bit7</th></tr>
<tr><td colspan="6">DSCP</td><td colspan="2">-</td></tr>
</table>

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 21-8 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 21-11 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

Default behavior

None

Impact on communication

If any entry is added when an access list with no entries set is being applied to an interface, the IP packets received on the applicable 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. When `255.255.255.255` is entered for the source address wildcard and the destination address wildcard, `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. `dscp` cannot be set at the same time as `tos` or `precedence`.
4. The protocol name, ah or 51 (in decimal) cannot be set in *<protocol>* as the detection condition for filtering.

Related commands

ip access-group

ip access-list resequence

permit (ip access-list extended)

remark

deny (ip access-list standard)

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

Syntax

To set or change information:

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

To delete information:

no *<seq>*

Input mode

`(config-std-nacl)`

Parameters

<seq>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

   If conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specify an IPv4 address.

To specify all IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   - *<ipv4> [<ipv4 wildcard>]* specification:

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

     For `[`*<ipv4 wildcard>*`]`, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address. If omitted, the filter condition is a perfect match of *<ipv4>*.

   - `host` *<ipv4>* specification:

     The filter condition is a perfect match of *<ipv4>*.

   - `any` specification:

     The IPv4 address is not included 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 any entry is added when an access list with no entries set is being applied to an interface, the IP packets received on the applicable 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. When `255.255.255.255` is entered as the address wildcard, `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

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

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is TCP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is UDP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is ICMP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

To delete information:

no *<seq>*

Input mode

`(config-ipv6-acl)`

Parameters

<seq>

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.

   See *Table 21-2 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`.

   - *<source ipv6>/<length>* specification:

     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.

   - `host` *<source ipv6>* specification:

     The filter condition is a perfect match of *<source ipv6>*.

   - `any` specification:

     The source IPv6 address is not used as filter conditions.

   <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 21-3 Port names that can be specified for TCP* and *Table 21-5 Port names that can be specified for UDP (IPv6)*.

   If `eq` is specified, the filter condition is a perfect 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`.

   - *<destination ipv6>/<length>* specification:

     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.

   - `host` *<destination ipv6>* specification:

     The filter condition is a perfect match of *<destination ipv6>*.

   - `any` specification:

     The destination IPv6 address is not included 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 21-3 Port names that can be specified for TCP* and *Table 21-5 Port names that can be specified for UDP (IPv6)*.

   If `eq` is specified, the filter condition is a perfect 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.

The 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.)

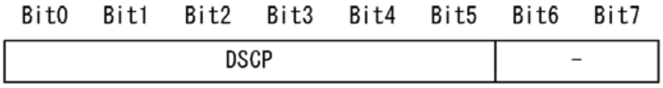
2. Range of values:

   Specify 0 to 255 in decimal.

dscp *<dscp>*

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

The value is compared with the first 6 bits in the TOS field of the received packet.



1. Default value when this parameter is omitted:

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

2. Range of values:

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

   For details about the DSCP names that can be specified, see *Table 21-8 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 21-12 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

Default behavior

None

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If *nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`/0` is entered as the source address and the destination address, `any` is displayed.
2. If *nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`/128` is entered as the source address and the destination address, `host` *nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn*`:`*nnnn* is displayed.
3. The IPv6 address is displayed in abbreviated form.

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:

[*<seq>*] 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 } [*<ethernet type>*] [vlan *<vlan id>*] [user-priority *<priority>*] [class *<class>* [mask *<class mask>*]]

To delete information:

no *<seq>*

Input mode

`(config-ext-macl)`

Parameters

<seq>

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`.

   - *<source mac>* *<source mac mask>* specification:

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

     For *<source mac mask>*, specify a mask in MAC address format that sets bits that permit an arbitrary value in the MAC address.

   - `host` *<source mac>* specification:

     The filter condition is a perfect match of *<source mac>*.

   - `any` specification:

     The source MAC address is not included 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}

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`, or `pvst-plus-bpdu`.

   - *<destination mac> <destination mac mask>* specification:

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

     For *<destination mac mask>*, specify a mask in MAC address format that sets bits that permit an arbitrary value in the MAC address.

   - `host` *<destination mac>* specification:

     The filter condition is a perfect match of *<destination mac>*.

   - `any` specification:

     The destination MAC address is not included as a filter condition.

   - `bpdu` specification:

     Sets BPDU control packets as a filter condition.

   - `cdp` specification:

     Sets CDP control packets as a filter condition.

   - `lacp` specification:

     Sets LACP control packets as a filter condition.

   - `lldp` specification:

     Sets LLDP control packets as a filter condition.

   - `oadp` specification:

     Sets OADP control packets as a filter condition.

   - `pvst-plus-bpdu` specification:

     Sets PVST+ control packets as a filter condition.

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

<ethernet type>

Specifies the Ethernet type number or the Ethernet type name.

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 21-9 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

Default behavior

None

Impact on communication

If any entry is added when an access list with no entries set is being applied to an interface, all packets received on the applicable 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. 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 21-10 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 functionality.

Syntax

To set information:

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

To delete information:

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

Input mode

`(config-if)`

Parameters

<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:

   Specify an access list name that is 4 to 31 characters.
   For details about the characters that can be specified, see *Specifiable values for parameters*.

{in | out}

Specifies Inbound or Outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

When an access list with at least one entry is 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 sides of an 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. The following table shows whether the setting is possible for each receiving-side flow detection mode.

Table 21-13 Whether the setting is possible for each receiving-side flow detection mode (IPv4)

Receiving-side flow detection mode	Whether the setting is possible	
	Ethernet	VLAN
layer2-1	N	N
layer2-2	Y	Y
layer2-3	Y	Y

Legend Y: Possible; N: Not possible

4. The following table shows whether the setting is possible for each sending-side flow detection mode.

Table 21-14 Whether the setting is possible for each sending-side flow detection mode (IPv4)

Sending-side flow detection mode	Whether the setting is possible	
	Ethernet	VLAN
layer2-1-out	N	N
layer2-2-out	Y	Y
layer2-3-out	Y	Y

Legend Y: Possible; N: Not possible

5. 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.
6. 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.
7. An access list that contains a VLAN parameter as a flow detection condition can be set on the outbound side if no tunneling ports have been set for the Ethernet interface for the switch.
8. An access list that contains a VLAN parameter as a flow detection condition can be set on the outbound side if tag translation has not been set for the target interface.
9. An access list can be set on the outbound side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the switch.
10. You can set an access list on the outbound side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.
11. The filter functionality does not support some packets. For details, see *1. Filters* in the *Configuration Guide Vol. 2*.

Related commands

ip access-list standard

ip access-list extended

ip access-list extended

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

This command sets an IPv4 packet filter.

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

Multiple filter conditions can be specified with one ID of the access list. Note that for the receiving-side Ethernet interface and the VLAN interface, up to 255 conditions can be specified, and for the sending-side, up to 127 conditions. For a Switch, a maximum of 512 access lists (for IPv4, IPv6, and MAC) can be created. A maximum of 1024 filter condition entries can be created.

Syntax

To set or change information:

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

To delete information:

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

Input mode

`(config)`

Parameters

<access list name>

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

The Switch enters config-ext-nacl mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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

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

Related commands

ip access-group

ip access-list resequence

deny (ip access-list extended)

permit (ip access-list extended)

remark

ip access-list resequence

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

Syntax

To set or change information:

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

Input mode

`(config)`

Parameters

<access list name>

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:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip access-list standard

ip access-list extended

ip access-list standard

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

This command sets an IPv4 address filter.

An IPv4 address filter filters packets based on IPv4 address.

Multiple filter conditions can be specified with one ID of the access list. Note that for the receiving-side Ethernet interface and the VLAN interface, up to 255 conditions can be specified, and for the sending-side, up to 127 conditions. For a Switch, a maximum of 512 access lists (for IPv4, IPv6, and MAC) can be created. A maximum of 1024 filter condition entries can be created.

Syntax

To set or change information:

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

To delete information:

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

Input mode

`(config)`

Parameters

<access list name>

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

The Switch enters config-std-nacl mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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

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

Related commands

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

Multiple filter conditions can be specified with one ID of the access list. Note that for the receiving-side Ethernet interface and the VLAN interface, up to 255 conditions can be specified, and for the sending-side, up to 127 conditions. For a Switch, a maximum of 512 access lists (for IPv4, IPv6, and MAC) can be created. A maximum of 1024 filter condition entries can be created.

Syntax

To set or change information:

ipv6 access-list *<access list name>*

To delete information:

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

Input mode

`(config)`

Parameters

<access list name>

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

The Switch enters config-ipv6-acl mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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

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 an access list name that is 4 to 31 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ipv6 access-list

ipv6 traffic-filter

Applies an IPv6 access list to an Ethernet interface or VLAN interface and enables the IPv6 filter functionality.

Syntax

To set information:

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

To delete information:

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

Input mode

`(config-if)`

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 an access list name that is 4 to 31 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

{ in | out }

Specifies Inbound or Outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

When an access list with at least one entry is 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 sides of an 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. The following table shows whether the setting is possible for each receiving-side flow detection mode.

Table 21-15 Whether the setting is possible for each receiving-side flow detection mode (IPv6)

Receiving-side flow detection mode	**Whether the setting is possible**	
	Ethernet	**VLAN**
layer2-1	N	N
layer2-2	N	N
layer2-3	Y	Y

Legend Y: Possible; N: Not possible

4. The following table shows whether the setting is possible for each sending-side flow detection mode.

Table 21-16 Whether the setting is possible for each sending-side flow detection mode (IPv6)

Sending-side flow detection mode	**Whether the setting is possible**	
	Ethernet	**VLAN**
layer2-1-out	N	N
layer2-2-out	N	N
layer2-3-out	Y	Y

Legend Y: Possible; N: Not possible

5. When an IPv6 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.
6. When an IPv6 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.
7. An access list that contains a VLAN parameter as a flow detection condition can be set on the outbound side if no tunneling ports have been set for the Ethernet interface for the switch.
8. An access list that contains a VLAN parameter as a flow detection condition can be set on the outbound side if tag translation has not been set for the target interface.
9. An access list can be set on the outbound side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the switch.
10. You can set an access list on the outbound side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.
11. The filter functionality does not support some packets. For details, see *1. Filters* in the *Configuration Guide Vol. 2*.

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 functionality.

Syntax

To set information:

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

To delete information:

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

Input mode

`(config-if)`

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 an access list name that is 4 to 31 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

{in | out}

Specifies Inbound or Outbound.

`in`: Inbound (Specifies the receiving side)

`out`: Outbound (Specifies the sending side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

When an access list with at least one entry is 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 sides of an 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. The following table shows whether the setting is possible for each receiving-side flow detection mode.

Table 21-17 Whether the setting is possible for each receiving-side flow detection mode (MAC)

Receiving-side flow detection mode	**Whether the setting is possible**	
	Ethernet	**VLAN**
layer2-1	Y	Y
layer2-2	N	N
layer2-3	N	N

Legend Y: Possible; N: Not possible

4. The following table shows whether the setting is possible for each sending-side flow detection mode.

Table 21-18 Whether the setting is possible for each sending-side flow detection mode (MAC)

Sending-side flow detection mode	**Whether the setting is possible**	
	Ethernet	**VLAN**
layer2-1-out	Y	Y
layer2-2-out	N	N
layer2-3-out	Y	Y

Legend Y: Possible; N: Not possible

5. 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.
6. 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.
7. An access list that contains a VLAN parameter as a flow detection condition can be set on the outbound side if no tunneling ports have been set for the Ethernet interface for the switch.
8. An access list that contains a VLAN parameter as a flow detection condition can be set on the outbound side if tag translation has not been set for the target interface.
9. An access list can be set on the outbound side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the switch.
10. You can set an access list on the outbound side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.
11. The filter functionality does not support some packets. For details, see *1. Filters* in the *Configuration Guide Vol. 2*.

Related commands

mac access-list extended

mac access-list extended

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

Multiple filter conditions can be specified with one ID of the access list. Note that for the receiving-side Ethernet interface and the VLAN interface, up to 255 conditions can be specified, and for the sending-side, up to 127 conditions. For a Switch, a maximum of 512 access lists (for IPv4, IPv6, and MAC) can be created. A maximum of 1024 filter condition entries can be created.

Syntax

To set or change information:

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

To delete information:

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

Input mode

```
(config)
```

Parameters

<access list name>

Specifies the identifier of the MAC filter that is to be set. The Switch enters config-ext-macl mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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

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 an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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:

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

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is TCP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is UDP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is ICMP

  [*<seq>*] 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>*] [class *<class>* [mask *<class mask>*]]

To delete information:

no *<seq>*

Input mode

`(config-ext-nacl)`

Parameters

<seq>

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| 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:

   - *<protocol>*:

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

     See *Table 21-1 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`.

   - *<source ipv4>* *<source ipv4 wildcard>* specification:

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

     For *<source ipv4 wildcard>*, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address.

   - `host` *<source ipv4>* specification:

     The filter condition is a perfect match of *<source ipv4>*.

   - `any` specification:

     The source IPv4 address is not included 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 21-3 Port names that can be specified for TCP* and *Table 21-4 Port names that can be specified for UDP (IPv4)*.

   If `eq` is specified, the filter condition is a perfect 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`.

   - *<destination ipv4>* *<destination ipv4 wildcard>* specification:

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

     For *<destination ipv4 wildcard>*, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address.

   - `host` *<destination ipv4>* specification:

     The filter condition is a perfect match of *<destination ipv4>*.

   - `any` specification:

     The destination IPv4 address is not included 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 21-3 Port names that can be specified for TCP* and *Table 21-4 Port names that can be specified for UDP (IPv4)*.

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

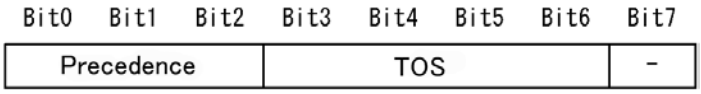
   If `range` is specified, the filter condition is in the range from *<destination port start>* to *<destination port end>*.

   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.



1. Default value when this parameter is omitted:

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

2. Range of values:

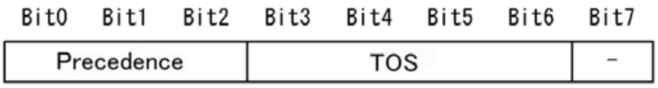
   Specify 0 to 15 (in decimal) or a TOS name.

For details about the TOS names that can be specified, see *Table 21-6 TOS names that can be specified*.

precedence *<precedence>*

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

The 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:

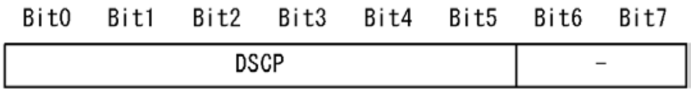
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see *Table 21-7 Precedence names that can be specified*.

dscp *<dscp>*

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

The 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 21-8 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.

Default value when this parameter is omitted:

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

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 21-11 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

Default behavior

None

Impact on communication

If any entry is added when an access list with no entries set is being applied to an interface, the IP packets received on the applicable 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. When `255.255.255.255` is entered for the source address wildcard and the

destination address wildcard, `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. `dscp` cannot be set at the same time as `tos` or `precedence`.
4. The protocol name, ah or 51 (in decimal) cannot be set in *<protocol>* as the detection condition for filtering.

Related commands

ip access-group

ip access-list resequence

deny (ip access-list extended)

remark

permit (ip access-list standard)

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

Syntax

To set or change information:

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

To delete information:

no *<seq>*

Input mode

`(config-std-nacl)`

Parameters

<seq>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

   If conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specify an IPv4 address.

To specify all IPv4 addresses, specify `any`.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   - *<ipv4> [<ipv4 wildcard>]* specification:

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

     For `[`*<ipv4 wildcard>*`]`, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address. If wildcards are omitted, the filter condition is a perfect match of *<ipv4>*.

   - *host <ipv4>* specification:

     The filter condition is a perfect match of *<ipv4>*.

   - `any` specification:

     The IPv4 address is not included 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 any entry is added when an access list with no entries set is being applied to an interface, the IP packets received on the applicable 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. When `255.255.255.255` is entered as the address wildcard, `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

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:

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

  [*<seq>*] permit {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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is TCP

  [*<seq>*] permit 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is UDP

  [*<seq>*] permit 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>*] [class *<class>* [mask *<class mask>*]]

- When the upper layer protocol is ICMP

  [*<seq>*] permit 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>*] [class *<class>* [mask *<class mask>*]]

To delete information:

no *<seq>*

Input mode

`(config-ipv6-acl)`

Parameters

<seq>

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.

   See *Table 21-2 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`.

   - *<source ipv6>/<length>* specification:

     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.

   - `host` *<source ipv6>* specification:

     The filter condition is a perfect match of *<source ipv6>*.

   - `any` specification:

     The source IPv6 address is not used as filter conditions.

   <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 21-3 Port names that can be specified for TCP* and *Table 21-5 Port names that can be specified for UDP (IPv6)*.

   If `eq` is specified, the filter condition is a perfect 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`.

   - *<destination ipv6>*`/`*<length>* specification:

     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.

   - `host` *<destination ipv6>* specification:

     The filter condition is a perfect match of *<destination ipv6>*.

   - `any` specification:

     The destination IPv6 address is not included 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 21-3 Port names that can be specified for TCP* and *Table 21-5 Port names that can be specified for UDP (IPv6)*.

   If `eq` is specified, the filter condition is a perfect 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.

The 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 TOS field.

The 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 21-8 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 21-12 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

Default behavior

None

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If `nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/0` is entered as the source address and the destination address, `any` is displayed.
2. If `nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/128` is entered as the source address and the destination address, `host nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn` is displayed.
3. The IPv6 address is displayed in abbreviated form.

Related commands

ipv6 traffic-filter

ipv6 access-list resequence

deny (ipv6 access-list)

remark

permit (mac access-list extended)

Specifies the conditions by which the MAC filter permits access.

Syntax

To set or change information:

[*<seq>*] permit {*<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 } [*<ethernet type>*] [vlan *<vlan id>*] [user-priority *<priority>*] [class *<class>* [mask *<class mask>*]]

To delete information:

no *<seq>*

Input mode

`(config-ext-macl)`

Parameters

<seq>

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`.

   - *<source mac>* *<source mac mask>* specification:

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

     For *<source mac mask>*, specify a mask in MAC address format that sets bits that permit an arbitrary value in the MAC address.

   - `host` *<source mac>* specification:

     The filter condition is a perfect match of *<source mac>*.

   - `any` specification:

     The source MAC address is not included 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 }

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`, or `pvst-plus-bpdu`.

   - *<destination mac> <destination mac mask>* specification:

     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.

   - `host` *<destination mac>* specification:

     The filter condition is a perfect match of *<destination mac>*.

   - `any` specification:

     The destination MAC address is not included as a filter condition.

   - `bpdu` specification:

     Sets BPDU control packets as a filter condition.

   - `cdp` specification:

     Sets CDP control packets as a filter condition.

   - `lacp` specification:

     Sets LACP control packets as a filter condition.

   - `lldp` specification:

     Sets LLDP control packets as a filter condition.

   - `oadp` specification:

     Sets OADP control packets as a filter condition.

   - `pvst-plus-bpdu` specification:

     Sets PVST+ control packets as a filter condition.

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

<ethernet type>

Specify the Ethernet type number or the Ethernet type name.

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 21-9 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

Default behavior

None

Impact on communication

If any entry is added when an access list with no entries set is being applied to an interface, all packets received on the applicable 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. 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 21-10 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

remark

Sets supplementary information for an access list. Access lists are available for IPv4 address filtering, IPv4 packet filtering, IPv6 filtering, and MAC filtering.

Syntax

To set or change information:

remark *<remark>*

To delete information:

no remark

Input mode

```
(config-ext-nacl)
(config-std-nacl)
(config-ipv6-acl)
(config-ext-macl)
```

Parameters

<remark>

Sets supplementary information according to input mode.

One line can be set for each access list. Entering new information overwrites the existing information.

1. Default value when this parameter is omitted:

   The initial value is null.

2. Range of values:

   Specify a character string that is no more than 64 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip access-list standard

ip access-list extended

ipv6 access-list

mac access-list extended

22. QoS

Names and values that can be specified
ip qos-flow-group
ip qos-flow-list
ip qos-flow-list resequence
ipv6 qos-flow-group
ipv6 qos-flow-list
ipv6 qos-flow-list resequence
limit-queue-length
mac qos-flow-group
mac qos-flow-list
mac qos-flow-list resequence
qos (ip qos-flow-list)
qos (ipv6 qos-flow-list)
qos (mac qos-flow-list)
qos-queue-group
qos-queue-list
remark
traffic-shape rate
control-packet user-priority

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 22-1 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 flow condition.

Protocol names (IPv6)

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

Table 22-2 Protocol names that can be specified (IPv6)

Protocol name	Applicable protocol number
gre	47
icmp	58
ipv6	All IP protocols
ospf	89

Protocol name	Applicable protocol number
pcp	108
pim	103
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 22-3 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)

Port name	Applicable port name and number
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)
lpd	Printer service (515)
nntp	Network News Transfer Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
pop3s	POP3 over TLS/SSL (995)
raw	Printer PDL Data Stream (9100)
shell	Remote commands (514)
smtp	Simple Mail Transfer Protocol (25)
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 22-4 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)

Port name	Applicable port name and number
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

Table 22-5 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)

Names and values that can be specified

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

TOS name

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

Table 22-6 TOS names that can be specified

TOS name	TOS value
max-reliability	2
max-throughput	4
min-delay	8
min-monetary-cost	1

TOS name	TOS value
normal	0

Precedence name

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

Table 22-7 Precedence names that can be specified

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

DSCP name

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

Table 22-8 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

DSCP name	DSCP value
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 22-9 Ethernet type names that can be specified

Ethernet type name	Ethernet value	Notes
appletalk	0x809b	
arp	0x0806	
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 22-10 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

Message name (ICMP)

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

Table 22-11 Message names that can be specified for ICMP (IPv4)

Message name	Message	Type	Code
administratively-prohibited	Administratively prohibited	3	13
alternate-address	Alternate address	6	Not specified
conversion-error	Datagram conversion	31	Not specified
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	Not specified
echo-reply	Echo reply	0	Not specified
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1

Message name	Message	Type	Code
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 22-12 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

Names and values that can be specified

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

ip qos-flow-group

Enables the QoS functionality by applying an IPv4 QoS flow list to an Ethernet interface or a VLAN 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)`

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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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. Up to 128 entries can be specified for each IPv4 QoS flow list that is applied to the inbound side.
3. If you specify a non-existent IPv4 QoS flow list name, this will be ignored. The IPv4 QoS flow list name is registered.
4. The following table shows whether the setting is possible for each receiving-side flow

detection mode.

Table 22-13 Whether the setting is possible for each receiving-side flow detection mode (IPv4)

Receiving-side flow detection mode	Whether the setting is possible	
	Ethernet	VLAN
layer2-1	N	N
layer2-2	Y	Y
layer2-3	Y	Y

Legend Y: Possible; N: Not possible

5. 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.
6. 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.
7. When an IPv4 QoS flow list is to be applied to a VLAN interface, the list can be set if no VLAN parameters exist as a flow detection condition.
8. The QoS functionality does not support some packets. For details, see *3. Flow Control* in the *Configuration Guide Vol. 2*.

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 512 IPv4, IPv6, and MAC QoS flow lists can be created for a Switch. A maximum of 1024 flow detection and action specification entries can be created.

Syntax

To set or change 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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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

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:

   4 to 31 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip qos-flow-list

ipv6 qos-flow-group

Enables the QoS functionality by applying an IPv6 QoS flow list to an Ethernet interface or a VLAN interface.

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)`

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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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. Up to 64 entries can be specified for each IPv6 QoS flow list that is applied to the inbound side.
3. If you specify a non-existent IPv6 QoS flow list name, this will be ignored. The IPv6 QoS flow list name is registered.
4. The following table shows whether the setting is possible for each receiving-side flow

detection mode.

Table 22-14 Whether the setting is possible for each receiving-side flow detection mode (IPv6)

Receiving-side flow detection mode	**Whether the setting is possible**	
	Ethernet	**VLAN**
layer2-1	N	N
layer2-2	N	N
layer2-3	Y	Y

Legend Y: Possible; N: Not possible

5. 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.

6. 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.

7. When an IPv6 QoS flow list is to be applied to a VLAN interface, the list can be set if no VLAN parameters exist as a flow detection condition.

8. The QoS functionality does not support some packets. For details, see *3. Flow Control* in the *Configuration Guide Vol. 2*.

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 512 IPv4, IPv6 and MAC QoS flow lists can be created for a Switch. A maximum of 1024 flow detection and action specification entries can be created.

Syntax

To set or change 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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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

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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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

```
ipv6 qos-flow-list resequence
```

Related commands

ipv6 qos-flow-list

limit-queue-length

Sets for a Switch the maximum send queue length of a physical port.

If this command is omitted or if setting information is deleted, the send queue length is set to 64.

This command is used to set basic operating conditions for the hardware. You must restart the Switch after you change the settings.

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:

   64, 128, or 728 is specified.

Default behavior

64 is used as the send queue length for a port on a Switch.

Impact on communication

The Switch must be restarted. Communication via the Switch stops until the restart processing has been completed.

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.

Notes

1. When this command is entered, the message below is displayed. Before entering another configuration command, save the settings and restart the Switch.

   Please execute the reload command after save,

   because this command becomes effective after reboot.

2. Before setting this command, use the `qos-queue-list` command to set scheduling mode PQ. The PQ scheduling mode cannot be set from other scheduling modes.

   This also applies when 64 is set as the send queue length.

3. If information is deleted by using the `no` command, there will be no scheduling mode limitations.

4. When 64 has been set as the send queue length by using the `limit-queue-length`

command, the send queue length is as follows:

Queues 1 to 8: 64

5. When 128 has been set as the send queue length by using the `limit-queue-length` command, the send queue length is as follows:

   Queues 1 to 4: 128

   Queues 5 to 8: 0

6. When 728 has been set as the send queue length by using the `limit-queue-length` command, the send queue length is as follows:

   Queue 1: 728

   Queue 2: 64

   Queues 3 to 8: 0

   At this time, use the `flowcontrol` command to configure the sending of pause packets.

Related commands

qos-queue-list

flowcontrol

mac qos-flow-group

Enables the QoS functionality by applying a MAC QoS flow list to an Ethernet interface or a VLAN 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)`

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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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. Up to 128 entries can be specified for each MAC QoS flow list that is applied to the inbound side.
3. If a non-existent MAC QoS flow list name is set, no operation is performed. The MAC QoS flow list name is registered.
4. The following table shows whether the setting is possible for each receiving-side flow

detection mode.

Table 22-15 Whether the setting is possible for each receiving-side flow detection mode (MAC)

Receiving-side flow detection mode	Whether the setting is possible	
	Ethernet	**VLAN**
layer2-1	Y	Y
layer2-2	N	N
layer2-3	N	N

Legend Y: Possible; N: Not possible

5. 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.
6. 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.
7. When an MAC QoS flow list is to be applied to a VLAN interface, the list can be set if no VLAN parameters exist as a flow detection condition.
8. The QoS functionality does not support some packets. For details, see *3. Flow Control* in the *Configuration Guide Vol. 2*.

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 512 IPv4, IPv6 and MAC QoS flow lists can be created for a Switch. A maximum of 1024 flow detection and action specification entries can be created.

Syntax

To set or change 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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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

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:

   4 to 31 characters can be specified. For details about the characters that can be specified, 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:

`[<seq>] qos {flow detection condition}[action specification]`

- Flow detection conditions

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

{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>*] [class *<class>* [mask *<class mask>*]]

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>*] [class *<class>* [mask *<class mask>*]]

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>*] [class *<class>* [mask *<class mask>*]]

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>*] [class *<class>* [mask *<class mask>*]]

- Action specification

action [cos *<cos>*] [replace-user-priority *<priority>*] [replace-dscp *<dscp>*]

To delete information:

no *<seq>*

Input mode

`(config-ip-qos)`

Parameters

<seq>

Specifies 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 | 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:

   - *<protocol>*:

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

     See *Table 22-1 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`.

   - *<source ipv4>* *<source ipv4 wildcard>* specification:

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

     For *<source ipv4 wildcard>*, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address.

   - `host` *<source ipv4>* specification:

     The flow detection condition is a perfect match of *<source ipv4>*.

   - `any` specification:

     The source IPv4 address is not included 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 22-3 Port names that can be specified for TCP* and *Table 22-4 Port names that can be specified for UDP (IPv4)*.

   If `eq` is specified, the flow detection condition is a perfect 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`.

   - *<destination ipv4>* *<destination ipv4 wildcard>* specification:

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

     For *<destination ipv4 wildcard>*, specify a wildcard in IPv4 address format that sets bits that permit an arbitrary value in an IPv4 address.

   - `host` *<destination ipv4>* specification:

     The flow detection condition is a perfect match of *<destination ipv4>*.

   - `any` specification:

     The destination IPv4 address is not included 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 22-3 Port names that can be specified for TCP* and *Table 22-4 Port names that can be specified for UDP (IPv4)*.

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

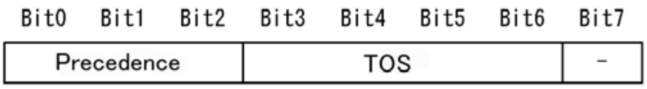
   If `range` is specified, the flow detection condition is in the range from *<destination port start>* to *<destination port end>*.

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

tos *<tos>*

Sets four 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 22-6 TOS names that can be specified*.

precedence <*precedence*>

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

The value is compared with the first 3 bits in the TOS field of the sent or received packet.

<table>
<tr><td>Bit0</td><td>Bit1</td><td>Bit2</td><td>Bit3</td><td>Bit4</td><td>Bit5</td><td>Bit6</td><td>Bit7</td></tr>
<tr><td colspan="3">Precedence</td><td colspan="4">TOS</td><td>-</td></tr>
</table>

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 22-7 Precedence names that can be specified*.

dscp <*dscp*>

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

The value is compared with the first 6 bits in the TOS field of the received packet.

<table>
<tr><td>Bit0</td><td>Bit1</td><td>Bit2</td><td>Bit3</td><td>Bit4</td><td>Bit5</td><td>Bit6</td><td>Bit7</td></tr>
<tr><td colspan="6">DSCP</td><td colspan="2">-</td></tr>
</table>

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 22-8 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 22-11 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

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 Switch.

1. Default value when this parameter is omitted:

   The default CoS values are set. For details about the default Cos values, see *3.7.1 CoS value* in the *Configuration Guide Vol. 2*.

2. Range of values:

   Specify 0 to 7 in decimal.

replace-user-priority *<priority>*

Specifies the value for rewriting the user priority.

The user priority of the received packet is replaced with the specified *<priority>* value.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

replace-dscp *<dscp>*

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the specified *<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 22-8 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. When `255.255.255.255` is entered for the source address wildcard and the destination address wildcard, `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. `dscp` cannot be set at the same time as `tos` or `precedence`.
4. When `cos` and `replace-user-priority` are set for the `action` parameter at the same time, the user priority is replaced with the value set for `cos`.
5. The protocol name, ah or 51 (in decimal) cannot be set in *<protocol>* as the detection

condition for flow detection.

Related commands

ip qos-flow-list

ip qos-flow-group

ip qos-flow-list resequence

remark

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>*] [class *<class>* [mask *<class mask>*]]
- 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>*] [class *<class>* [mask *<class mask>*]]
- 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>*] [class *<class>* [mask *<class mask>*]]
- 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>*] [class *<class>* [mask *<class mask>*]]
- Action specification

  action [cos *<cos>*] [replace-user-priority *<priority>*] [replace-dscp *<dscp>*]

To delete information:

no *<seq>*

Input mode

`(config-ipv6-qos)`

Parameters

<seq>

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:

   - *<protocol>*:

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

     See *Table 22-2 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`.

   - *<source ipv6>*`/`*<length>* specification:

     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.

   - `host` *<source ipv6>* specification:

     The flow detection condition is a perfect match of *<source ipv6>*.

   - `any` specification:

     The source IPv6 address is not included 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 22-3 Port names that can be specified for TCP* and *Table 22-5 Port names that can be specified for UDP (IPv6)*.

   If `eq` is specified, the flow detection condition is a perfect 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 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`.

   - *<destination ipv6>/<length>* specification:

     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.

   - `host` *<destination ipv6>* specification:

     The flow detection condition is a perfect match of *<destination ipv6>*.

   - `any` specification:

     The destination IPv6 address is not included 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 22-3 Port names that can be specified for TCP* and *Table 22-5 Port names that can be specified for UDP (IPv6)*.

   If `eq` is specified, the flow detection condition is a perfect 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>*.

traffic-class *<traffic class>*

Specifies the traffic class field value.

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

1. Default value when this parameter is omitted:

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

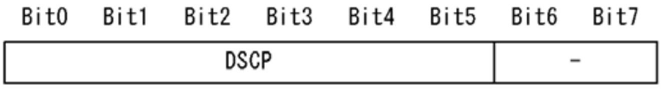
2. Range of values:

   Specify 0 to 255 in decimal.

dscp *<dscp>*

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

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



1. Default value when this parameter is omitted:

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

2. Range of values:

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

   For details about the DSCP names that can be specified, see *Table 22-8 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 22-12 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

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 Switch.

1. Default value when this parameter is omitted:

   The default CoS values are set. For details about the default Cos values, see *3.7.1 CoS value* in the *Configuration Guide Vol. 2*.

2. Range of values:

   Specify 0 to 7 in decimal.

replace-user-priority *<priority>*

Specifies the value for rewriting the user priority.

The user priority of the received packet is replaced with the specified *<priority>* value.

1. Default value when this parameter is omitted:

None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

replace-dscp *<dscp>*

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the specified *<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 22-8 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. 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. `traffic-class` and `dscp` cannot be set at the same time.
4. When `cos` and `replace-user-priority` are specified for the `action` parameter at the same time, the user priority is replaced with the value specified for `cos`.

Related commands

ipv6 qos-flow-list

ipv6 qos-flow-group

ipv6 qos-flow-list resequence

remark

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 }[*<ethernet type>*] [vlan *<vlan id>*] [user-priority *<priority>*] [class *<class>* [mask *<class mask>*]]

- Action specification

  action [cos *<cos>*] [replace-user-priority *<priority>*]

To delete information:

no *<seq>*

Input mode

`(config-mac-qos)`

Parameters

<seq>

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`.

   - *<source mac> <source mac mask>* specification:

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

     For *<source mac mask>*, specify a mask in MAC address format that sets bits that permit an arbitrary value in the MAC address.

   - `host` *<source mac>* specification:

     The flow detection condition is a perfect match of *<source mac>*.

- `any` specification:

  The source MAC address is not included 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 }

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`, or `pvst-plus-bpdu`.

   - *<destination mac> <destination mac mask>* specification:

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

     For *<destination mac mask>*, specify a mask in MAC address format that sets bits that permit an arbitrary value in the MAC address.

   - `host` *<destination mac>* specification:

     The flow detection condition is a perfect match of *<destination mac>*.

   - `any` specification:

     The destination MAC address is not included as a flow detection condition.

   - `bpdu` specification:

     Sets BPDU control packets as a flow detection condition.

   - `cdp` specification:

     Sets CDP control packets as a flow detection condition.

   - `lacp` specification:

     Sets LACP control packets as a flow detection condition.

   - `lldp` specification:

     Sets LLDP control packets as a flow detection condition.

   - `oadp` specification:

     Sets OADP control packets as a flow detection condition.

   - `pvst-plus-bpdu` specification:

     Sets PVST+ control packets as a flow detection condition.

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

<ethernet type>

Specify the Ethernet type number or the Ethernet type name.

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.

   Note, however, that 0x0000 is set for a value equal to or smaller than 0x05ff.

   For details about the Ethernet type names that can be specified, see *Table*

22-9 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.

class *<class>* [mask *<class mask>*]

Specifies the user class and class mask.

For *<class mask>*, specify a class mask in which the bits corresponding to those in *<class>* that are to be compared are set.

If *<class mask>* is omitted, all bits are compared.

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.

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 Switch.

1. Default value when this parameter is omitted:

   The default CoS values are set. For details about the default Cos values, see *3.7.1 CoS value* in the *Configuration Guide Vol. 2*.

2. Range of values:

   Specify 0 to 7 in decimal.

replace-user-priority *<priority>*

Specifies the value for rewriting the user priority.

The user priority of the received packet is replaced with the specified *<priority>* value.

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.

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 22-10 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. When `cos` and `replace-user-priority` are set for the `action` parameter at the same time, the user priority is replaced with the value set for `cos`.
4. The parameters set by using this command are valid only for relay packets. Therefore, the set parameters are not valid for packets addressed to the device and packets originated by the device.

Related commands

mac qos-flow-list

mac qos-flow-group

mac qos-flow-list resequence

remark

qos-queue-group

Sets QoS queue list information for an interface (physical port).

Syntax

To set information:

qos-queue-group *<QoS queue list name>*

To delete information:

no qos-queue-group

Input mode

`(config-if)`

Parameters

<QoS queue list name>

Specifies the QoS queue list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 31 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

`PQ` is set as the scheduling mode.

Impact on communication

If the scheduling mode is changed by setting the QoS queue list name, all the remaining packets queued in the send queue of the line will be cleared.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the scheduling mode is changed by setting the QoS queue list name, all the remaining packets queued in the send queue in the changed interface will be cleared. During the clear processing, a new packet cannot 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 queue list name is specified by using the `qos-queue-group` command, PQ is used as the scheduling mode.

Related commands

qos-queue-list

interface gigabitethernet

interface tengigabitethernet

qos-queue-list

Sets the scheduling mode in QoS queue list information. A maximum of 52 lists can be created for a Switch.

Syntax

To set or change information:

qos-queue-list *<QoS queue list name>* { pq | wrr [*<Packet1> <Packet2> <Packet3> <Packet4> <Packet5> <Packet6> <Packet7> <Packet8>*] | wfq [min-rate1 *<Min rate1>*] [min-rate2 *< Min rate2>*] [min-rate3 *< Min rate3>*] [min-rate4 *< Min rate4>*] [min-rate5 *< Min rate5>*] [min-rate6 *< Min rate6>*] [min-rate7 *< Min rate7>*] [min-rate8 *< Min rate8>*] | 2pq+6wrr *< Packet1> < Packet2> < Packet3> < Packet4> < Packet5> < Packet6>* }

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:

   4 to 31 characters can be specified. For details about the characters that can be specified, see *Specifiable values for parameters*.

{ pq | wrr [*<Packet1> <Packet2> <Packet3> <Packet4> <Packet5> <Packet6> <Packet7> <Packet8>*] | wfq [min-rate1 *<Min rate1>*] [min-rate2 *< Min rate2>*] [min-rate3 *< Min rate3>*] [min-rate4 *< Min rate4>*] [min-rate5 *< Min rate5>*] [min-rate6 *< Min rate6>*] [min-rate7 *< Min rate7>*] [min-rate8 *< Min rate8>*] | 2pq+6wrr *< Packet1> < Packet2> < Packet3> < Packet4> < Packet5> < Packet6>* }

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 at eight queues for each physical port. If there are packets in multiple queues, the packets with the highest priority queue number are always sent first (for example, packets in queue 8 are sent first, followed the packets in queue 7, and so on, until queue 1 is reached).

wrr [*<Packet1> <Packet2> <Packet3> <Packet4> <Packet5> <Packet6> <Packet7> <Packet8>*]

Sets round robin or weighted (number of packets) round robin. The number of queues is fixed at eight queues for each physical port. If the *<Packet>* setting is omitted, round robin is used. Packets are sent by looking at the queue in order. Regardless of the queue length, the number of packets is controlled so that packets are distributed evenly. When *<Packet>* is set, weighted (number of packets) round robin is used. If there are packets in multiple queues, packets are sent according to the number of packets set for *<Packet>* >as the queues are looked at in order. 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.

   Note, however, that all *<Packet>* values can be omitted. If they are omitted, round robin is used.

2. Range of values:

   <Packet>: 1 to 15

wfq [min-rate1 *<Min rate1>*] [min-rate2 *< Min rate2>*] [min-rate3 *< Min rate3>*] [min-rate4 *< Min rate4>*] [min-rate5 *< Min rate5>*] [min-rate6 *< Min rate6>*] [min-rate7 *< Min rate7>*] [min-rate8 *< Min rate8>*]

Weighted fair queuing. The number of queues is fixed at eight queues for each physical port. The minimum bandwidth, which is set for each queue as *<Min rate>*, is sent for packets. Note that a number from 1 to 8 suffixed to *<Min rate>* indicates a queue number.

1. Default value when this parameter is omitted:

   <Min rate>: None.(A minimum bandwidth is not set.)

2. Range of values:

   `min-rate` *<Min rate>*: See the table below.

   You can specify k (default), M, or G for the unit of the value.

   { *<Min rate>* | *<Min rate>*M | *<Min rate>*G }

   Set *<Min rate>* values so that their total value does not exceed the line bandwidth.

Table 22-16 Range of values for the minimum bandwidth

Setting unit[#1]	**Setting range**	**Increment**
Gbit/s	1 G to 10 G	1 Gbit/s
Mbit/s	1 M to 10000 M	1 Mbit/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: When setting a value of 1000 k or more, specify the value in 100 k increments (1000, 1100, 1200...10000000).

#3: When setting a value less than 1000 k, specify the value in 64 k increments (64, 128, 192...960).

2pq+6wrr *< Packet1> < Packet2> < Packet3> < Packet4> < Packet5> < Packet6>*

Top-priority queues and weighted (number of packets) round robin. The number of queues is fixed at eight queues for each physical port. If there are packets in top-priority queue 8, the applicable packets are sent at the highest priority. The applicable packets in queue 7 are sent at the next priority after queue 8. If there are no packets in queues 8 and 7, packets are sent according to the number of bytes set for *<Packet>* for queues 6 to 1. A number from 1 to 6 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 setting the QoS queue list name set in the `qos-queue-group` command, all the remaining packets queued in the send queue of the line will be cleared.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the scheduling mode is changed by setting the QoS queue list name set in the `qos-queue-group` command, all the remaining packets queued in the send queue in the changed interface will be cleared. During the clear processing, a new packet cannot be queued. You need to be careful if you logged in via a network.
2. WFQ does not correctly work when the line status is in the half duplex mode. Use the full duplex mode.
3. If WFQ is set, there might be a maximum error of 10% between the set minimum bandwidth and the actual value.
4. To use port bandwidth control and scheduling of QoS queue list information at the same time, set PQ as the scheduling mode.
5. If `wfq` is selected as the scheduling mode, *<Min rate>* must be set for the queues that will be used.
6. When the bandwidth is set in Mbit/s (*<Mbit/s>*`M`) or Gbit/s (*<Gbit/s>*`G`), the value is displayed in kbit/s for `show running-config and show startup-config`.

Related commands

qos-queue-group

remark

Sets 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.

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:

   Specify a character string that is no more than 64 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ip qos-flow-list

ipv6 qos-flow-list

mac qos-flow-list

traffic-shape rate

Sets the bandwidth by setting port bandwidth control for an interface (physical port) to limit the send bandwidth.

Syntax

To set or change information:

traffic-shape rate { *<kbit/s>* | *<Mbit/s>*M | *<Gbit/s>*G }

To delete information:

no traffic-shape rate

Input mode

`(config-if)`

Parameters

rate { *<kbit/s>* | *<Mbit/s>*M | *<Gbit/s>*G }

Sets port bandwidth control. Using this functionality limits the total-line send bandwidth to the 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 22-17 Setting range for port bandwidth control

Setting unit[#1]	**Setting range**	**Increment**
Gbit/s	1 G to 10 G	1 Gbit/s
Mbit/s	1 M to 10000 M	1 Mbit/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: When setting a value of 1000 k or more, specify the value in 100 k increments (1000, 1100, 1200...10000000).

#3: When setting a value less than 1000 k, specify the value in 64 k increments (64, 128, 192...960).

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. There might be a maximum error of 10% between the set port bandwidth value and the actual value.
2. When the line status is half duplex, port bandwidth control is not supported.
3. To use port bandwidth control and scheduling of QoS queue list information at the same time, set PQ as the scheduling mode.
4. When the bandwidth is set in Mbit/s (*<Mbit/s>*`M`) or Gbit/s (*<Gbit/s>*`G`), the value is displayed in kbit/s for `show running-config and show startup-config`.
5. When the set bandwidth for port bandwidth control exceeds the line speed, the port bandwidth is not controlled.

Related commands

interface gigabitethernet

interface tengigabitethernet

control-packet user-priority

Specifies the user priority in the VLAN tags of frames spontaneously sent by a Switch. If this command is not set or if information is deleted, 7 is used as the user priority of frames spontaneously sent.

Syntax

To set or change information:

control-packet user-priority { layer-2 *<User-priority>* | layer-3 *<User-priority>* | layer-2 *<User-priority>* layer-3 *<User-priority>* }

To delete information:

no control-packet user-priority

Input mode

`(config)`

Parameters

{ layer-2 *<User-priority>* | layer-3 *<User-priority>* | layer-2 *<User-priority>* layer-3 *<User-priority>* }

Specifies the user priority of frames spontaneously sent by a Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 0 to 7. 7 is used as the user priority if no value is specified.

Default behavior

7 is used as the user priority of frames spontaneously sent by a Switch.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

Part 9: Layer 2 Authentication

23. Common to Layer 2 Authentication

authentication arp-relay

Forwards ARP packets received from unauthenticated terminals to other ports.

Syntax

To set information:

```
authentication arp-relay
```

To delete information:

```
no authentication arp-relay
```

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting this command, you must set one of the following commands for the applicable port in advance:
   - dot1x port-control
   - web-authentication port
   - mac-authentication port

Related commands

dot1x system-auth-control

dot1x port-control

web-authentication system-auth-control

web-authentication port

web-authentication redirect enable

mac-authentication system-auth-control

mac-authentication port

authentication auto-logout strayer

Cancels the authentication when the Web-authenticated or MAC-authenticated terminal is detected to have moved to a port where Web authentication or MAC-based authentication is not set.

Syntax

To set information:

authentication auto-logout strayer

To delete information:

no authentication auto-logout strayer

Input mode

```
(config)
```

Parameters

None

Default behavior

Even if the Web-authenticated or MAC-authenticated terminal is detected to have moved to a port where Web authentication or MAC-based authentication is not set, the authentication is not canceled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. IEEE 802.1X is outside the scope of this command.
2. For the terminal that has move during Web authentication (while waiting for RADIUS authentication, etc.), when the authentication is completed and the terminal is again detected to have moved, the authentication is canceled.
3. If the terminal has moved while the MAC-based authentication is being processed (while waiting for RADIUS authentication, etc.) or suspended, the authentication is cancelled.
4. If VLAN of the terminal changes when the terminal moves, the move of the terminal might not be detected until broadcast packets are received from the terminal that has moved. In addition, if the Switch does not have the IP address of VLAN interface after the move, the move of the terminal might not be detected even if broadcast packets are received from the terminal that has moved.

Related commands

None

authentication force-authorized enable

When the following state exists for all Layer 2 authentications, a terminal subject to authentication that requested authentication is forcibly changed to the authenticated state.

- RADIUS authentication is specified but there is no response from the designated RADIUS server

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 functionality, as it can pose security problems.
2. In dynamic VLAN mode, assign the native VLAN of the applicable port 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. This functionality operates when the RADIUS authentication only is set. If multiple authentication methods are set, the forced authentication functionality does not operate.
4. Register the general-use RADIUS server information or the authentication RADIUS server information. For details, see *5. Overview of Layer 2 Authentication Functionality* in the *Configuration Guide Vol. 2*.
5. The private Trap of forced authentication is sent regardless of the `snmp-server traps` command setting.

Related commands

aaa authentication dot1x

aaa authentication mac-authentication

aaa authentication web-authentication

dot1x port-control

dot1x system-auth-control

dot1x radius-server

radius-server

mac-authentication port

mac-authentication system-auth-control

mac-authentication radius-server

web-authentication port

web-authentication system-auth-control

web-authentication radius-server

authentication force-authorized vlan

In dynamic VLAN mode of Web authentication and MAC-based authentication, and port-based authentication (dynamic) for IEEE 802.1X authentication, set this command to assign a post-authentication VLAN when forced authentication is performed on the applicable port.

Syntax

To set or change information:

authentication force-authorized vlan *<VLAN ID>*

To delete information:

no authentication force-authorized vlan

Input mode

`(config-if)`

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, however, that the default VLAN (`VLAN ID = 1`) cannot be set.

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

1. The `authentication force-authorized vlan` command is valid only when the `authentication force-authorized enable` command is set.
2. When this command is set or deleted, a terminal or a currently authenticated user operates in the VLAN that was accommodated by the previous setting. The values set for the `authentication force-authorized vlan` command take effect after re-authentication or the next authentication.
3. This functionality operates when the RADIUS authentication only is set. If multiple authentication methods are set, the forced authentication functionality does not operate.
4. Register the general-use RADIUS server information or the authentication RADIUS server information. For details, see *5. Overview of Layer 2 Authentication Functionality* in the *Configuration Guide Vol. 2*.

Related commands

authentication force-authorized enable

vlan mac-based

authentication ip access-group

Applies the IPv4 access list specified with this command to the IP packets received from unauthenticated terminals, and forwards the IP packet that matches (permits) the list to other ports.

The IP packet that matches (permits) the IPv4 access list specified with this command is not the target of URL redirection.

Syntax

To set information:

authentication ip access-group *<access list name>*

To delete information:

no authentication ip access-group

Input mode

`(config-if)`

Parameters

<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. One IPv4 packet filter identifier can be specified by using this parameter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

IPv4 packets received from unauthenticated terminals are not forwarded.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. One access list name can be set for a Switch by using this command.
2. When setting this command, you must set one of the following commands for the applicable port in advance:
   - dot1x port-control
   - web-authentication port
   - mac-authentication port

Related commands

dot1x system-auth-control

dot1x port-control

web-authentication system-auth-control

web-authentication port

web-authentication redirect enable

mac-authentication system-auth-control

mac-authentication port

ip access-list extended

authentication logout linkdown

If the `no authentication logout linkdown` command is set, even if the link of a port to which authenticated terminals belong goes down, the authentication status of the terminals is not cleared.

Syntax

To set information:

```
no authentication logout linkdown
```

To delete information:

```
authentication logout linkdown
```

Input mode

`(config-if)`

Parameters

None

Default behavior

If the link of a port to which authenticated terminals belong goes down, the authentication status of the terminals is cleared.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

dot1x port-control

dot1x system-auth-control

mac-authentication port

mac-authentication system-auth-control

shutdown

web-authentication port

web-authentication system-auth-control

authentication max-user (global)

Sets the maximum number of terminals that can be authenticated on a Switch 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>

Specify the maximum number of terminals that can be authenticated on a Switch 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 Switch 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. Also, the authentication might be canceled by re-authentication or roaming.
2. The maximum number of terminals that can be authenticated on a Switch 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 Switch, no more terminals can be authenticated on that Switch.
   - The maximum number of terminals that can be authenticated on the applicable port in Web authentication dynamic VLAN mode, MAC-based authentication dynamic VLAN mode, and IEEE 802.1X port-based authentication (dynamic) mode, which are set concurrently, is restricted to 1000. This is due to a restriction on MAC VLANs.

authentication max-user (global)

Related commands

dot1x system-auth-control

mac-authentication system-auth-control

web-authentication system-auth-control

authentication max-user (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)`

Parameters

<count>

Specify 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 each 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. Also, the authentication might be canceled by re-authentication or roaming.
2. The maximum number of terminals that can be authenticated on a Switch 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 Switch, no more terminals can be authenticated on that Switch.
3. The maximum number of terminals that can be authenticated on the applicable port in Web authentication dynamic VLAN mode, MAC-based authentication dynamic VLAN mode, and IEEE 802.1X port-based authentication (dynamic) mode, which

are set concurrently, is restricted to 1000. This is due to a restriction on MAC VLANs.

Related commands

dot1x port-control

mac-authentication port

web-authentication port

24. IEEE 802.1X

Correspondence between configuration commands and authentication modes

The following table describes IEEE 802.1X authentication modes in which IEEE 802.1X configuration commands can be set.

Table 24-1 Configuration commands and IEEE 802.1X authentication modes

	IEEE 802.1X authentication modes[#4]	
	Port-based authentication	
Command name	**(static)**	**(dynamic)**
aaa accounting dot1x	Y	Y
aaa authentication dot1x	Y	Y
authentication arp-relay[#1]	Y	Y
authentication ip access-group[#1]	Y	Y
dot1x authentication	Y	Y
dot1x auto-logout	Y	Y
dot1x force-authorized eapol	Y	Y
dot1x ignore-eapol-start	Y	Y
dot1x logging enable	Y	Y
dot1x max-req	Y	Y
dot1x multiple-authentication	Y	Y
dot1x port-control[#2]	Y	Y
dot1x radius-server dead-interval	Y	Y
dot1x radius-server host	Y	Y
dot1x reauthentication	Y	Y
dot1x supplicant-detection	Y	Y
dot1x system-auth-control	Y	Y
dot1x timeout keep-unauth[#3]	Y	Y
dot1x timeout quiet-period	Y	Y
dot1x timeout reauth-period	Y	Y
dot1x timeout server-timeout	Y	Y

	IEEE 802.1X authentication modes#4	
	Port-based authentication	
Command name	**(static)**	**(dynamic)**
dot1x timeout supp-timeout	Y	Y
dot1x timeout tx-period	Y	Y

Legend

Y: The command operates according to the settings.

--: The command can be entered, but it will have no effect.

N: The command cannot be entered.

#1

For details about command input formats, see *23. Common to Layer 2 Authentication*.

#2

The specification of this command affects the switching of authentication modes.

#3

The setting for this command is applied only to an interface in single-mode authentication submode.

#4

For details such as a description of the authentication modes, see the *Configuration Guide Vol. 2*.

aaa accounting dot1x

Sends IEEE 802.1X accounting information to the accounting server.

Syntax

To set information:

aaa accounting dot1x default start-stop group radius

To delete information:

no aaa accounting dot1x default

Input mode

`(config)`

Parameters

default

Sets the default accounting method of a Switch.

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.

group radius

The RADIUS server is used as the accounting server.

Default behavior

A notification is not sent to the accounting server.

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

aaa authentication dot1x

dot1x system-auth-control

radius-server host or dot1x radius-server host

aaa authentication dot1x

Sets an IEEE 802.1X authentication method group.

If `default` is set, one entry can be set. If an authentication method list name is specified, a maximum of four entries can be set.

Syntax

To set or change information:

aaa authentication dot1x default *<Method>*

aaa authentication dot1x *<List name>* group *<Group name>*

To delete information:

no aaa authentication dot1x {default | *<List name>*}

Input mode

`(config)`

Parameters

default *<Method>*

Sets the default authentication method of a Switch. For *<Method>*, specify `group radius`.

group radius

IEEE 802.1X authentication is performed by a RADIUS server. The RADIUS server that can be used is an IEEE 802.1X RADIUS server or a general-use RADIUS server.

<List name>

Sets the name of an authentication method list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

   We recommend that you use an upper-case letter for the first character.

   However, you cannot use the following character strings:

   - at mark (`@`)
   - `default` or a character string beginning with `default`

group *<Group name>*

IEEE 802.1X authentication is performed by a RADIUS server. The RADIUS server to use is a RADIUS server group. Specify the RADIUS server group name set by the `aaa group server radius` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

None

Impact on communication

When you change the setting of this command, the Switch clears the authentication status of the terminals to be affected.

- When the Switch default is added, the authentication status is not cleared.
- When the Switch default is changed or deleted, the authentication status of the terminals authenticated with the Switch default is cleared.
- When the authentication method list is added, the authentication status of terminals on ports specifying the corresponding authentication method list is cleared. (If the authentication method list that is set on the ports is not set in this command, authentication is performed with the Switch default.)
- When the authentication method list is changed or deleted, the authentication status of the terminals authenticated with the corresponding authentication method list is cleared.

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. If this command is not set, the RADIUS server cannot be used for IEEE 802.1X authentication.

Related commands

aaa group server radius

dot1x authentication

dot1x system-auth-control

radius-server host or dot1x radius-server host

dot1x authentication

Sets the name of an authentication method list for the port-based authentication method.

Syntax

To set or change information:

dot1x authentication *<List name>*

To delete information:

no dot1x authentication

Input mode

`(config-if)`

Parameters

<List name>

Sets the authentication method list name set by using the `aaa authentication dot1x` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*. (with the exception of the at mark (@))

   We recommend that you use an upper-case letter for the first character.

Default behavior

IEEE 802.1X authentication is performed by using the default values of the Switch.

Impact on communication

Authentication of a terminal for a port whose authentication method list name has been changed is canceled.

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command cannot be set when the `web-authentication user-group` command has been set.
4. If the authentication method list name set by using this command does not match the authentication method list name set by using the `aaa authentication dot1x` command, the default settings of the Switch are used.

Related commands

aaa authentication dot1x

dot1x authentication

dot1x port-control

dot1x system-auth-control

dot1x auto-logout

The `no dot1x auto-logout` command disables the setting to automatically cancel authentication when no frame is received from a terminal authenticated by IEEE 802.1X for a certain period of time.

Syntax

To set information:

```
no dot1x auto-logout
```

To delete information:

```
dot1x auto-logout
```

Input mode

`(config)`

Parameters

None

Default behavior

Authentication is automatically canceled if no frames are received from a terminal authenticated by IEEE 802.1X for a certain period of time.

Impact on communication

After the `no dot1x auto-logout` command is set, authentication is not automatically canceled if no frames are received from a terminal authenticated by IEEE 802.1X for a certain period of time.

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

dot1x port-control

dot1x system-auth-control

mac-address-table aging-time

dot1x force-authorized eapol

Sends according to the IEEE 802.1X forced authentication settings the EAPOL-Success response packet from the Switch to the terminal to be authenticated when its status has been forcibly changed to authentication authorized.

Syntax

To set information:

```
dot1x force-authorized eapol
```

To delete information:

```
no dot1x force-authorized eapol
```

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command is applied to operations for forced authentication permission by setting the `authentication force-authorized enable` command.

Related commands

authentication force-authorized enable

dot1x ignore-eapol-start

Sets the Switch not to issue EAP-Request/Identity packets in response to EAPOL-Start from a supplicant.

Syntax

To set information:

dot1x ignore-eapol-start

To delete information:

no dot1x ignore-eapol-start

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.
4. This command can be set only on an interface on which the `dot1x reauthentication` command has been set and the `dot1x supplicant-detection` command without the `disable` parameter set has been set.
5. This command cannot be set on an interface on which the `dot1x supplicant-detection` command with the `disable` parameter set has been set.
6. If this command has been set, you cannot use the `no dot1x reauthentication` command to set no re-authentication.

Related commands

dot1x reauthentication

dot1x supplicant-detection

dot1x system-auth-control

dot1x port-control

dot1x logging enable

For IEEE 802.1X authentication, enables operation log information to be output to a syslog server.

Syntax

To set information:

dot1x logging enable

To delete information:

no dot1x logging enable

Input mode

`(config)`

Parameters

None

Default behavior

Operation log information is not output to a syslog server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

dot1x system-auth-control

logging event-kind

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 *<Counts>*

To delete information:

no dot1x max-req

Input mode

```
(config-if)
```

Parameters

<Counts>

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 (times)

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. 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 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.

If terminal authentication mode is set as the authentication submode, single mode is used as the submode. Single mode authentication permits connection of only one terminal. When multiple terminals are connected, the status of the interface that has been set changes to no authentication.

Syntax

To set information:

dot1x multiple-authentication

To delete information:

no dot1x multiple-authentication

Input mode

`(config-if)`

Parameters

None

Default behavior

The authentication submode is single mode.

Impact on communication

If the authentication submode is changed, the authentication status of the interface that has been set is initialized. As a result, authenticated terminals must be re-authenticated. 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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only when `auto` is set for the `dot1x port-control` command.
4. If the authentication submode is changed, the authentication status of the interface that has been set is initialized. As a result, authenticated terminals must be re-authenticated.
5. Behavior of a terminal configured by using the `mac-address-table static` command is as follows:
    - When this command has not been set (single mode)

      Communication is impossible as long as a terminal subject to authentication has not been authenticated successfully.

- When this command has been set (terminal authentication mode)

  Regardless of the authentication status, if `auto` is set for the `dot1x port-control` command, communication is always possible.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x port-control

Sets the port-control status for an interface that has been set. Entering this command also enables the IEEE 802.1X port-based authentication functionality.

Syntax

To set or change information:

dot1x port-control {auto | force-authorized | force-unauthorized}

To delete information:

no dot1x port-control

Input mode

`(config-if)`

Parameters

{auto | force-authorized | force-unauthorized}

auto

IEEE 802.1X authentication processing is performed. The authentication result determines whether communication for the terminals connected to the interface is possible.

force-authorized

IEEE 802.1X authentication is not performed, and communication by the terminals connected to the interface that has been set is always possible. This parameter can be set only if the mode for port-based authentication (static) is single mode.

force-unauthorized

IEEE 802.1X authentication is not performed, and communication by the terminals connected to the interface that has been set is never possible. This parameter can be set only if the mode for port-based authentication (static) is single mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `auto`, `force-authorized`, or `force-unauthorized`

Default behavior

The port-based authentication functionality is disabled.

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for

the authentication mode in which the command's settings are operable.

3. When port-based authentication (static) is used, set the following commands for the same interface:
   - dot1x port-control auto
   - switchport mode access
   - switchport access
4. When port-based authentication (dynamic) is used, set the following commands for the same interface:
   - dot1x port-control auto
   - switchport mode mac-vlan
5. When the `authentication ip access-group` command or the a`uthentication arp-relay` command has been set for the applicable port, this command can be deleted if the following condition exists:
   - `web-authentication port` or `mac-authentication port` has been set.
6. If the `dot1x multiple-authentication` command has not been set, the authentication submode is single mode.

Related commands

dot1x system-auth-control

dot1x multiple-authentication

switchport mode

switchport access

switchport mac

dot1x radius-server dead-interval

Configures the timer for monitoring automatic restoration to the primary IEEE 802.1X authentication RADIUS server from the IEEE 802.1X authentication RADIUS server.

The primary IEEE 802.1X authentication RADIUS server is restored when either of the following occurs: The current server (the destination for RADIUS authentication requests in operation) switches to a valid secondary IEEE 802.1X authentication RADIUS server, or when all servers are disabled, the monitoring timer starts and the period of time set by this command elapses (when the monitoring timer expires).

Syntax

To set or change information:

dot1x radius-server dead-interval *<Minutes>*

To delete information:

no dot1x radius-server dead-interval

Input mode

```
(config)
```

Parameters

<Minutes>

Configures the timer for monitoring automatic restoration to the primary IEEE 802.1X authentication RADIUS server from the secondary IEEE 802.1X authentication RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 1440 (minutes)

   If 0 is set, RADIUS authentication requests are always initiated from the primary IEEE 802.1X authentication RADIUS server.

Default behavior

The primary IEEE 802.1X authentication RADIUS server is automatically restored 10 minutes after the current server switches to the secondary IEEE 802.1X authentication RADIUS server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

1. If the secondary IEEE 802.1 authentication RADIUS server is operating as the current server, and if the value of the monitoring timer is changed, the progress to that time is used as the judgment value and the result is applied.
2. If this command configuration is deleted after the monitoring timer starts, the monitoring timer counter continues without being reset and runs for 10 minutes (default value).

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. If three or more IEEE 802.1X authentication RADIUS servers are configured and the current server switches to another IEEE 802.1X authentication RADIUS server after the monitoring timer starts, the monitoring timer is not reset and continues to run.
4. In general, when the monitoring timer has started, it does not reset until it expires. However, as exceptions, it resets in the following cases:
    - When `dot1x radius-server dead-interval 0` is set by using the `dot1x radius-server dead-interval` command
    - When information about the IEEE 802.1X authentication RADIUS server running as the current server is deleted by using the `dot1x radius-server host` command
    - When the `clear radius-server` operation command is executed
5. If the monitoring timer expires while the authentication sequence is being executed on a terminal subject to authentication, restoration of the primary IEEE 802.1X authentication RADIUS server is not performed until the executed authentication sequence is completed.

Related commands

aaa authentication dot1x

dot1x port-control

dot1x system-auth-control

dot1x radius-server host

dot1x radius-server host

Configures the RADIUS server used for IEEE 802.1X.

Syntax

To set or change information:

dot1x radius-server host {*<ipv4 address>* | *<ipv6 address>*} [auth-port *<port>*] [acct-port *<port>*] [timeout *<seconds>*] [retransmit *<retries>*] [key *<string>*]

To delete information:

no dot1x radius-server host {*<ipv4 address>* | *<ipv6 address>*}

Input mode

`(config)`

Parameters

{*<ipv4 address>* | *<ipv6 address>*}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 address of the RADIUS server in colon notation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <ipv4 address>: IPv4 unicast address

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   <ipv6 address>: IPv6 global unicast address

   ::2 to fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff, fec0:: to feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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:

   The period of time set by using the `radius-server timeout` command is

used. If no period is set, the initial value is 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:

   The number of times set by using the `radius-server retransmit` command is used. If no value is set, the initial value is 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 the `radius-server key` command is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Specify with 64 or fewer characters. For details about the characters that can be specified, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The RADIUS server settings registered by using the `radius-server host` command are used.

If the `radius-server host` command is not registered, authentication cannot be performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. When this command is set, the setting information of the RADIUS server referenced by IEEE 801.X authentication has priority over the information set by the `radius-server host` command (the settings of the `radius-server host` command are not applied). For details about the settings of general-use RADIUS server information and the IEEE 802.1X authentication RADIUS server information, see *Configuration Guide Vol. 2*.
4. A maximum of 4 IEEE 802.1X authentication RADIUS servers can be specified for each Switch.
5. `127.*.*.*` cannot be set as an IPv4 address.

6. If the `key` parameter is omitted and the `radius-server key` command is not set, the RADIUS server is disabled.
7. If multiple IEEE 802.1X authentication RADIUS servers are configured, the address displayed first by using the `show radius-server` operation command is the address of the primary general-use RADIUS server. The primary IEEE 802.1X authentication RADIUS server is used as the initial current server (the destination for RADIUS authentication requests during operation).

   If a failure occurs on the primary IEEE 802.1X authentication RADIUS server, the current server switches to the next effective IEEE 802.1X authentication RADIUS server (the secondary RADIUS server). For details about automatic restoration of the primary IEEE 802.1X authentication RADIUS server, see the description of the `dot1x radius-server dead-interval` command.
8. If a RADIUS server with an IP address that matches has already been registered in the general-use RADIUS server configuration, other authentication-specific RADIUS server configuration, or the RADIUS server group configuration, all these parameters are replaced by the new commands that were entered automatically.

Related commands

aaa authentication dot1x

dot1x port-control

dot1x system-auth-control

dot1x reauthentication

After successful IEEE 802.1X authentication, this command sets whether a supplicant is to be re-authenticated. When this command is in effect, `EAP-Request/Identity` packets for re-authentication are sent at the interval set by using the `dot1x timeout reauth-period` command to a supplicant as a prompt for supplicant re-authentication.

Syntax

To set information:

dot1x reauthentication

To delete information:

no dot1x reauthentication

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.
4. If the `dot1x ignore-eapol-start` command has been set, 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

Sets the behavior when a new terminal is detected after the terminal authentication mode has been set to an authentication submode.

Syntax

To set or change information:

dot1x supplicant-detection {disable | shortcut | auto}

To delete information:

no dot1x supplicant-detection

Input mode

`(config-if)`

Parameters

{disable | shortcut | auto}

Specifies the behavior when a new terminal is detected after terminal authentication mode has been set to an authentication submode.

disable

If terminals detected in the corresponding port exist, this parameter prevents EAP-Request/Identity transmission processing for detecting a new terminal when the authentication submode has been set to terminal authentication mode. Specify this parameter if a supplicant operates abnormally if the authentication sequence is omitted in order to decrease switch load.

If this parameter is specified, authentication processing for a supplicant for which authentication cannot be initiated from the terminal cannot be started.

shortcut

Sends EAP-Request/Identity packets regularly in multicast routing for detecting a new terminal when the authentication submode is set to terminal authentication mode. Also, to reduce the load, the authentication sequence of an authenticated terminal is omitted. Specify this parameter for a supplicant that is unable to initiate authentication from a terminal.

If this parameter is specified, some supplicants might not operate correctly and communication is temporarily stopped.

auto

Suppresses EAP-Request/Identity transmission processing for detecting a new terminal when the authentication submode is set to terminal authentication mode, and sends EAP-Request/Identity packets in unicast routing when an ARP/IP frame is received from a new terminal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   disable, shortcut, auto

Default behavior

`shortcut` is used as the operation when a new terminal is detected.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.
4. This command is valid only if the `dot1x multiple-authentication` command has been set.
5. `disable` cannot be set for the `dot1x supplicant-detection` command on an interface on 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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
2. If the EAPOL forwarding functionality has been set, this command fails and IEEE 802.1X is not enabled.
3. If the `aaa authentication dot1x` command has not been set, a RADIUS server cannot be used for IEEE 802.1X authentication.

Related commands

l2protocol-tunnel eap

aaa authentication dot1x

dot1x timeout keep-unauth

Sets the period of time (in seconds) for maintaining the communication-disabled state of the interface if two or more terminals are connected to an interface on which the single-mode authentication submode is set. After the time set by using this command elapses, an authenticated terminal must be re-authenticated.

Syntax

To set or change information:

dot1x timeout keep-unauth *<Seconds>*

To delete information:

no dot1x timeout keep-unauth

Input mode

`(config-if)`

Parameters

<Seconds>

Sets the period of time (in seconds) for maintaining the communication-disabled state when single mode is set as authentication submode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535 (seconds)

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. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.
4. The value set for this command is applied only to an interface in single-mode authentication submode.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x timeout keep-unauth

dot1x multiple-authentication

dot1x timeout quiet-period

Specifies the period of time (in seconds) for maintaining the unauthenticated state on the applicable interface after an IEEE 802.1X authentication failure. During this period, no EAPOL packets are sent and received EAPOL packets are ignored. Also, no authentication is performed.

Syntax

To set or change information:

dot1x timeout quiet-period *<Seconds>*

To delete information:

no dot1x timeout quiet-period

Input mode

`(config-if)`

Parameters

<Seconds>

Specifies the period of time (in seconds) for maintaining the unauthenticated state.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535 (seconds)

Default behavior

60 seconds is used as the period for maintaining the unauthenticated state.

Impact on communication

None

When the change is applied

When the Switch enters an unauthenticated state due to an authentication failure.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x timeout reauth-period

Specifies the interval (in seconds) for re-authenticating a supplicant after a successful IEEE 802.1X authentication. EAP-Request/Identify packets for re-authentication are sent to the supplicant at the interval set by using this command as a prompt for supplicant re-authentication.

Syntax

To set or change information:

dot1x timeout reauth-period *<Seconds>*

To delete information:

no dot1x timeout reauth-period

Input mode

`(config-if)`

Parameters

<Seconds>

Specifies the interval (in seconds) for re-authenticating a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535 (seconds)

Default behavior

3600 seconds is used as the interval for re-authenticating a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.
- When a terminal is authenticated successfully at the authentication level when there are no authenticated terminals.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.
4. This command takes effect only if re-authentication has been set by using the `dot1x reauthentication` command.
5. For the parameter, set a value greater than the value set by using the `dot1x timeout tx-period` command.

Related commands

dot1x timeout tx-period

dot1x reauthentication

dot1x system-auth-control

dot1x port-control

dot1x timeout server-timeout

Specifies the time (in seconds) to wait for a response, including the time required for retransmitting a response to an authentication server.

Syntax

To set or change information:

dot1x timeout server-timeout *<Seconds>*

To delete information:

no dot1x timeout server-timeout

Input mode

`(config-if)`

Parameters

<Seconds>

Specifies the time (in seconds) to wait for a response.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535 (seconds)

Default behavior

30 seconds is used as the time to wait for a response.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.

Related commands

dot1x system-auth-control

dot1x port-control

dot1x timeout supp-timeout

Specifies the time (in seconds) to wait for a response from a supplicant for an EAP-Request packet sent to a supplicant. If no response is received during the specified period, the EAP-Request packet is retransmitted.

Syntax

To set or change information:

dot1x timeout supp-timeout *<Seconds>*

To delete information:

no dot1x timeout supp-timeout

Input mode

`(config-if)`

Parameters

<Seconds>

Specifies the time (in seconds) to wait for a response from a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535 (seconds)

Default behavior

30 seconds is used as the time to wait for a response from a supplicant.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.

Related commands

dot1x system-auth-control

dot1x max-req

dot1x port-control

dot1x timeout tx-period

Specifies the interval (in seconds) for sending EAP-Request/Identity packets when IEEE 802.1X is valid.

Syntax

To set or change information:

dot1x timeout tx-period *<Seconds>*

To delete information:

no dot1x timeout tx-period

Input mode

`(config-if)`

Parameters

<Seconds>

Specifies the interval (in seconds) for sending EAP-Request/Identity packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535 (seconds)

Default behavior

30 seconds is used as the interval for sending EAP-Request/Identity packets.

Impact on communication

None

When the change is applied

- When the operating timer times out (the value of the timer becomes 0).
- When the `clear dot1x auth-state` operation command is executed to cancel authentication at the authentication level or the switch level.

Notes

1. All IEEE 802.1X settings take effect when the `dot1x system-auth-control` command is set.
2. See *Table 24-1 Configuration commands and IEEE 802.1X authentication modes* for the authentication mode in which the command's settings are operable.
3. This command takes effect only if the `dot1x port-control` command has been set.
4. 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

25. Web Authentication

Correspondence between configuration commands and authentication modes

The following table describes Web authentication modes in which Web authentication configuration commands can be set.

Table 25-1 Configuration commands and Web authentication modes

Command name	Web authentication modes[#3]	
	Fixed VLAN Mode	Dynamic VLAN Mode
aaa accounting web-authentication	Y	Y
aaa authentication web-authentication	Y	Y
aaa authentication web-authentication end-by-reject	Y	Y
authentication arp-relay[#1]	Y	Y
authentication ip access-group[#1]	Y	Y
web-authentication authentication	Y	Y
web-authentication auto-logout	Y	Y
web-authentication html-fileset	Y	Y
web-authentication ip address	Y	Y
web-authentication jump-url	Y	Y
web-authentication logging enable	Y	Y
web-authentication logout ping tos-windows	Y	Y
web-authentication logout ping ttl	Y	Y
web-authentication logout polling count	Y	--
web-authentication logout polling enable	Y	--
web-authentication logout polling interval	Y	--
web-authentication logout polling retry-interval	Y	--
web-authentication max-timer	Y	Y
web-authentication port[#2]	Y	Y
web-authentication prefilter	Y	Y

Command name	Web authentication modes[#3]	
	Fixed VLAN Mode	Dynamic VLAN Mode
web-authentication radius-server dead-interval	Y	Y
web-authentication radius-server host	Y	Y
web-authentication redirect-mode	Y	Y
web-authentication redirect enable	Y	Y
web-authentication redirect polling	Y	Y
web-authentication redirect queries	Y	Y
web-authentication redirect target	Y	Y
web-authentication roaming	--	Y
web-authentication static-vlan roaming	Y	--
web-authentication system-auth-control	Y	Y
web-authentication user-group	Y	Y
web-authentication user replacement	Y	Y
web-authentication web-port	Y	Y

Legend

Y: The command operates according to the settings.

--: The command can be entered, but it will have no effect.

N: The command cannot be entered.

#1

For details about command input formats, see *23. Common to Layer 2 Authentication*.

#2

The specification of this command affects the switching of authentication modes.

#3

For details such as a description of the authentication modes, see the *Configuration Guide Vol. 2*.

aaa accounting web-authentication

Sends accounting information for Web authentication to the accounting server.

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

default

Sets the default accounting method of a Switch.

start-stop

When a user logs in, an accounting start notification is sent to the accounting server. When a user logs out, a stop accounting notification is sent to the accounting server.

group radius

The RADIUS server is used as the accounting server.

Default behavior

A notification is not sent to the accounting server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

aaa authentication web-authentication

web-authentication system-auth-control

radius-server host or web-authentication radius-server host

aaa authentication web-authentication

Sets an authentication method group for Web authentication.

If the first specified method fails, the second specified method is used. You can change how authentication works when the first method failed by using the `aaa authentication web-authentication end-by-reject` command.

If `default` is set, one entry can be set. If an authentication method list name is specified, a maximum of four entries can be set.

Syntax

To set or change information:

aaa authentication web-authentication default *<Method>* [*<Method>*]

aaa authentication web-authentication *<List name>* group *<Group name>*

To delete information:

no aaa authentication web-authentication {default | *<List name>*}

Input mode

`(config)`

Parameters

default *<Method>* [*<Method>*]

Sets the default authentication method of a Switch. You cannot specify the same *<Method>* more than once.

For *<Method>*, specify `group radius` or `local`.

group radius

Web authentication is performed by a RADIUS server. The RADIUS server that can be used is a Web authentication RADIUS server or a general-use RADIUS server.

local

Local authentication is performed. The internal Web authentication DB is used.

<List name>

Sets the name of an authentication method list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

   We recommend that you use an upper-case letter for the first character.

   However, you cannot use the following character strings:

   - at mark (`@`)
   - `default` or a character string beginning with `default`
   - `end-by-reject` or a character string beginning with `end-by-reject`

group *<Group name>*

Web authentication is performed by a RADIUS server. The RADIUS server to use is a RADIUS server group. Specify the group name set by the `aaa group server` radius command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

User authentication is performed by using the internal Web authentication DB instead of using the RADIUS server.

Impact on communication

When you change the Switch default, the Switch clears the authentication status of the terminals authenticated with the authentication method of the Switch default.

When you change the setting of the authentication method list, the Switch clears the authentication status of the terminals authenticated with the corresponding authentication method list.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. Enabling of this command requires a separate authentication setting for the RADIUS server.
4. The forced authentication functionality for Web authentication operates when only RADIUS authentication is set. If multiple authentication methods are set, the forced authentication functionality does not operate.

Related commands

aaa authentication web-authentication end-by-reject

aaa group server radius

radius-server host or web-authentication radius-server host

web-authentication system-auth-control

web-authentication user-group

web-authentication authentication

aaa authentication web-authentication end-by-reject

Terminates authentication if login authentication is denied. If the authentication fails due to communication not being possible, such as unresponsive RADIUS server, the next authentication method specified by the `aaa authentication web-authentication` command is used to perform authentication.

Syntax

To set information:

aaa authentication web-authentication end-by-reject

To delete information:

no aaa authentication web-authentication end-by-reject

Input mode

`(config)`

Parameters

None

Default behavior

If authentication is denied, regardless of the reason for failure, the next authentication method specified by the `aaa authentication web-authentication` command is used to perform authentication.

Impact on communication

The authenticated status of a terminal authenticated with the Web authentication functionality is cleared.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
2. This command is only valid for authentication methods specified by the `aaa authentication web-authentication` command.

Related commands

aaa authentication web-authentication

web-authentication authentication

Sets the name of an authentication method list for the port-based authentication method.

Syntax

To set or change information:

web-authentication authentication *<List name>*

To delete information:

no web-authentication authentication

Input mode

`(config-if)`

Parameters

<List name>

Specify the authentication method list name set by using the `aaa authentication web-authentication` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters* (with the exception of the at mark (`@`)).
   We recommend that you use an upper-case letter for the first character.

Default behavior

Web authentication uses the default values of the Switch.

Impact on communication

Authentication of a terminal for a port whose authentication method list name has been changed is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. This command cannot be set when the `web-authentication user-group` command has been set.
4. If the name of the authentication method list set by using the `web-authentication authentication` command does not match the name of the authentication method list set by using the `aaa authentication web-authentication` command, the Switch default is used.

Related commands

aaa authentication web-authentication

web-authentication system-auth-control

web-authentication port

web-authentication auto-logout

The `no web-authentication auto-logout` command disables the setting for automatic authentication logout when it is detected that the status that frames have not been received from a terminal authenticated via Web authentication for a certain period of time.

Syntax

To set information:

```
no web-authentication auto-logout
```

To delete information:

```
web-authentication auto-logout
```

Input mode

`(config)`

Parameters

None

Default behavior

An authentication is automatically logged out if no frames are received from a terminal authenticated via Web authentication for a certain period of time.

Impact on communication

After the `no web-authentication auto-logout` command has been set, an authentication is not automatically logged out even if it is detected that no frames have been received from a terminal authenticated via Web authentication for a certain period of time.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

web-authentication system-auth-control

web-authentication port

mac-address-table aging-time

web-authentication html-fileset

Sets a custom file name for the Web authentication page displayed for each port.

Syntax

To set or change information:

web-authentication html-fileset *<Name>*

To delete information:

no web-authentication html-fileset

Input mode

`(config-if)`

Parameters

<Name>

Specify the custom file set name registered on the Switch by using the `set web-authentication html-files` operation command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 16 characters. Specifiable characters are upper-case alphanumeric characters.

Default behavior

The basic Web authentication page is displayed when a user logs in.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. To set this command, set the `web-authentication port` command for the applicable port in advance.

Related commands

web-authentication port

web-authentication system-auth-control

web-authentication ip address

Configure an IP address and a domain name to be used exclusively for Web authentication. When the Web authentication IP address has been set by using this command, you can log in from an unauthenticated terminal or log out from an authenticated terminal by using the same IP address on the switch.

Syntax

To set or change information:

web-authentication ip address *<IP address>* [fqdn *<FQDN>*]

To delete information:

no web-authentication ip address

Input mode

`(config)`

Parameters

<IP address>

Sets the Web authentication IP address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Sets the IPv4 address (dot notation).

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   IP address of a subnet that does not overlap a VLAN interface set for the Switch

fqdn *<FQDN>*

Use a fully qualified domain name (FQDN) for the domain name.

1. Default value when this parameter is omitted:

   Only *<IP address>* is used.

2. Range of values:

   Specify a string consisting of 1 to 255 characters. The first character must be an alphabetical character. Subsequent characters can be alphanumeric characters, periods (.), and hyphens (-).

   (It is possible to enter other characters, but use only the characters mentioned above.)

Default behavior

The IP address of an pre-authentication VLAN is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. When this setting is used, an IP address must be set for the pre-authentication VLAN.
4. To use the Web authentication IP address on a port in fixed VLAN mode or dynamic VLAN mode, you must set `authentication arp-relay`.
5. After this command is set or deleted, a user who is in the process of being authenticated must log in again.

Related commands

web-authentication system-auth-control

web-authentication port

authentication arp-relay

web-authentication jump-url

Specifies the URL of a page to be automatically displayed after displaying the page indicating successful login and the time required for jumping to the URL.

Syntax

To set or change information:

web-authentication jump-url { *<url>* | original } [delay *<seconds>*]

To delete information:

no web-authentication jump-url

Input mode

```
(config)
```

Parameters

{ *<url>* | original }

<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.)

original

If you start the authentication by using the URL redirect functionality, the page indicating successful login is displayed, and then the page of the pre-redirect URL is displayed.

If you start the authentication by directly specifying the Web authentication IP address or the IP address of the Switch, only the page indicating successful login is displayed after successful authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For *<url>*, enclose a character string consisting of 1 to 256 characters in double quotation marks. For the characters that can be specified, see *Specifiable values for parameters.*

   Example when specifying the URL:

   (config)# web-authentication jump-url "http://www.example.com/"

[delay *<seconds>*]

Specify the time required during jumping to the specified URL. (See the example below.)

1. Default value when this parameter is omitted:

   After five seconds, you are taken to the URL that has been set.

2. Range of values:

   0 to 60 (seconds)

   Example

   (config)# web-authentication jump-url "http://www.example.com/" delay 20

Default behavior

After successful authentication, only the page indicating successful login is displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. When replacing the login success page by using the `set web-authentication html-files` operation command, in the login 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 and the settings of this command. This causes the page specified by the URL to appear automatically after successful authentication.
4. If the login failed page is displayed due to a password input error or for other reasons and then you click the **login page** button to return to the login page, the specification of `original` becomes invalid, and the login success page remains displayed after successful authentication.
5. If you use the functionality for redirecting the user to an external Web server, note that the functionality depends on the external Web server. For details, see *8 Description of Web Authentication* in the *Configuration Guide Vol. 2*.
6. When specifying `original`, for details about the restrictions on the number of characters and character codes for the pre-redirect URL, see *8 Description of Web Authentication* in the *Configuration Guide Vol. 2*.

Related commands

web-authentication system-auth-control

web-authentication port

web-authentication logging enable

Enables the output of Web authentication operation log information to a syslog server.

Syntax

To set information:

```
web-authentication logging enable
```

To delete information:

```
no web-authentication logging enable
```

Input mode

`(config)`

Parameters

None

Default behavior

Operation log information is not output to a syslog server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

web-authentication system-auth-control

logging event-kind

web-authentication logout ping tos-windows

Sets the TOS value of a special frame used to log out from an authenticated terminal.

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 for the special frame used for logout.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 255

Default behavior

1 is set as the TOS value of the special frame.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. When a ping frame that meets all the following conditions is received, the authenticated terminal is logged out.
   - A ping frame is sent from an authenticated terminal to the Web authentication IP address.
   - The TTL value of the ping frame must match the TTL value specified by using the `web-authentication logout ping ttl` command.
   - The TOS value of the ping frame must match the TOS value set by using this command.

Related commands

web-authentication system-auth-control

web-authentication logout ping ttl

web-authentication logout ping ttl

Sets the TTL value of a special frame used to log out from an authenticated terminal.

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 the special frame used for logout.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

1 is set as the TTL value of the special frame.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. When a ping frame that meets all the following conditions is received, the authenticated terminal is logged out.
   - A ping frame is sent from an authenticated terminal to the Web authentication IP address.
   - The TTL value of the ping frame must match the TTL value specified by using this command.
   - The TOS value of the ping frame must match the TOS value set by using the `web-authentication logout ping tos-windows` command.

Related commands

web-authentication system-auth-control

web-authentication logout ping tos-windows

web-authentication logout polling count

Sets the number of times a Switch retransmits the monitoring frame when there is no response to a monitoring frame that periodically checks a connection status of authenticated terminals.

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 frame when there is no response to a monitoring frame.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10 (times)

Default behavior

The monitoring frame is retransmitted a maximum of three times.

Impact on communication

None

When the change is applied

The setting takes effect the first time no response is detected following the change of value.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If the link to a monitored terminal goes down before periodic monitoring by the functionality that monitors the connection of authenticated terminals arrives, the Switch stops monitoring the terminal and logs it out due to its link-down state.
4. When the specified maximum connection time (set by using the `web-authentication max-timer` command) expires, the Switch stops monitoring the applicable terminal and logs it out.
5. If the number of retransmissions when a no-response state is detected is set to the maximum, the number of monitoring frames increases proportionately with the number of authenticated users, overloading the Switch.

   Set the polling interval by using the following formula as a guide:

Polling condition:
(1) *polling-interval* > (2) *retransmission-interval* x (3) *number-of-retransmissions*

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

We recommend you use the default value for the number of retransmissions.

If a large value is set as the number of retransmissions, the difference between the polling interval and retransmission interval might increase depending on the retransmission frequency.

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 enable

The `no web-authentication logout polling enable` command disables the auto logout functionality executed when periodic connection monitoring detects that an authenticated terminal is not connected.

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

The connection of authenticated terminals is monitored according to the following conditions, and a terminal is automatically logged out if a no-connection state is detected.

- Polling interval

  The interval set by using the `web-authentication logout polling interval` command. 300 second is set by default.

- Retransmission interval

  The interval set by using the `web-authentication logout polling retry-interval` command. 1 second is set by default.

- Number of retransmissions

  The number of retransmissions set by using the `web-authentication logout polling count` command. Three retransmissions is set by default.

Impact on communication

When the `no web-authentication logout polling enable` command is set, connection is not monitored periodically. As a result, a terminal is not logged out automatically if it is disconnected.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If the link to a monitored terminal goes down before periodic monitoring by the functionality that monitors the connection of authenticated terminals arrives, the Switch stops monitoring the terminal and logs it out due to its link-down state.
4. When the specified maximum connection time (set by using the

`web-authentication max-timer` command) expires, the Switch stops monitoring the applicable terminal and logs it out.

5. The polling interval (set by using the `web-authentication logout polling interval` command) is the time between the receipt of ARP Reply from an authenticated terminal and the next polling monitoring.
6. If the number of retransmissions when a no-response state is detected is set to the maximum, the number of monitoring frames increases proportionately with the number of authenticated users, overloading the Switch.

   Set the polling interval by using the following formula as a guide:

   Polling condition:

   (1) *polling-interval* > (2) *retransmission-interval* x (3) *number-of-retransmissions*

   (1): web-authentication logout polling interval

   (2): web-authentication logout polling retry-interval

   (3): web-authentication logout polling count

   We recommend you use the default value for the number of retransmissions.

   If a large value is set as the number of retransmissions, the difference between the polling interval and retransmission interval might increase depending on the retransmission frequency.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling count

web-authentication logout polling interval

web-authentication logout polling retry-interval

web-authentication logout polling interval

Sets the polling interval of a monitoring frame that periodically monitors the connection status of an authenticated terminal.

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 polling interval of monitoring frames.

- Default value when this parameter is omitted:

  This parameter cannot be omitted.

- Range of values:

  60 to 86400 (seconds)

Default behavior

Monitoring frames are sent every 300 seconds to an authenticated terminal only if the automatic logout command (the `web-authentication logout polling enable` command) used with periodic monitoring has been set.

Impact on communication

None

When the change is applied

The setting takes effect from the next polling interval.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If the link to a monitored terminal goes down before periodic monitoring by the functionality that monitors the connection of authenticated terminals arrives, the Switch stops monitoring the terminal and logs it out due to its link-down state.
4. When the maximum connection time set by using the `web-authentication max-timer` command expires, the Switch stops monitoring the applicable terminal and logs it out.
5. The polling interval is the time between the receipt of ARP Reply from a target authenticated terminal and the next polling monitoring.
6. If the number of retransmissions when a no-response state is detected is set to the maximum, the number of monitoring frames increases proportionately with the

number of authenticated users, overloading the Switch.

Set the polling interval by using the following formula as a guide:

Polling condition:
(1) *polling-interval* > (2) *retransmission-interval* x (3) *number-of-retransmissions*

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

We recommend you use the default value for the number of retransmissions.

If a large value is set as the number of retransmissions, the difference between the polling interval and retransmission interval might increase depending on the retransmission frequency.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling count

web-authentication logout polling enable

web-authentication logout polling retry-interval

web-authentication logout polling retry-interval

Sets the interval between retransmissions of monitoring frames that periodically monitor the connection status of authenticated terminals when a no-response state is detected.

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 frames.

- Default value when this parameter is omitted:

  This parameter cannot be omitted.

- Range of values:

  1 to 10 (seconds)

Default behavior

1 second is set as the retransmission interval of monitoring frames.

Impact on communication

None

When the change is applied

The setting takes effect from the next retransmission interval.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If the link to a monitored terminal goes down before periodic monitoring by the functionality that monitors the connection of authenticated terminals arrives, the Switch stops monitoring the terminal and logs it out due to its link-down state.
4. When the maximum connection time set by using the `web-authentication max-timer` command expires, the Switch stops monitoring the applicable terminal and logs it out.
5. If the number of retransmissions when a no-response state is detected is set to the maximum, the number of monitoring frames increases proportionately with the number of authenticated users, overloading the Switch.

   Set the polling interval by using the following formula as a guide:

Polling condition:

(1) *polling-interval* > (2) *retransmission-interval* x (3) *number-of-retransmissions*

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

We recommend you use the default value for the number of retransmissions.

If a large value is set as the number of retransmissions, the difference between the polling interval and retransmission interval might increase depending on the retransmission frequency.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication port

web-authentication logout polling count

web-authentication logout polling enable

web-authentication logout polling interval

web-authentication max-timer

Sets the maximum connection time.

Syntax

To set or change information:

web-authentication max-timer { *<Minutes>* | infinity }

To delete information:

no web-authentication max-timer

Input mode

`(config)`

Parameters

{ *<Minutes>* | infinity }

Sets the maximum time (in minutes) that an authenticated user is allowed to be connected. After a user has logged in, if the time set by using this command elapses, the user is automatically logged out.

If `infinity` is set, there is no limit on the connection time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 1440 (minutes) 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. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If the value for the maximum connection time is either decreased or increased, the previous setting is applied to a user that is currently authenticated, and the current setting takes effect only from the next login.
4. The time on the Switch is not used for the connection time for Web authentication. Accordingly, if the date and time is changed by using the `set clock` operation command, the connection time is not affected.

Related commands

web-authentication system-auth-control

web-authentication max-timer

web-authentication auto-logout

web-authentication port

web-authentication port

Sets the authentication mode for ports.

Syntax

To set information:

```
web-authentication port
```

To delete information:

```
no web-authentication port
```

Input mode

`(config-if)`

Parameters

None

Default behavior

The Web authentication does not work on the corresponding port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

web-authentication html-fileset

web-authentication system-auth-control

authentication ip access-group

authentication arp-relay

web-authentication prefilter

Uses the `no web-authentication prefilter` command to set the Web authentication prefilter to disabled.

Syntax

To set information:

no web-authentication prefilter

To delete information:

web-authentication prefilter

Input mode

`(config)`

Parameters

None

Default behavior

The Web authentication prefilter is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.

Related commands

web-authentication system-auth-control

web-authentication radius-server dead-interval

Configures the timer for monitoring automatic restoration to the primary Web authentication RADIUS server from the Web authentication RADIUS server.

The primary Web authentication RADIUS server is restored when either of the following occurs: The current server (the destination for RADIUS authentication requests in operation) switches to a valid secondary Web authentication RADIUS server, or all servers are disabled, the monitoring timer starts, and the period of time set by this command elapses (when the monitoring timer expires).

Syntax

To set or change information:

web-authentication radius-server dead-interval *<Minutes>*

To delete information:

no web-authentication radius-server dead-interval

Input mode

`(config)`

Parameters

<Minutes>

Sets the timer for monitoring automatic restoration to the primary Wet authentication RADIUS server from the secondary Web authentication RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 1440 (minutes)

   If 0 is set, RADIUS authentication requests are always initiated from the primary Web authentication RADIUS server.

Default behavior

The primary Web authentication RADIUS server is automatically restored 10 minutes after the current server switches to the secondary Web authentication RADIUS server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

1. If the secondary Web authentication RADIUS server is operating as the current server, and if the value of the monitoring timer is changed, the progress to that time is used as the judgment value and the result is applied.
2. If this command configuration is deleted after the monitoring timer starts, the monitoring timer counter continues without being reset and runs for 10 minutes (default value).

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.

2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If three or more Web authentication RADIUS servers are configured and another Web authentication RADIUS server becomes the current server after the monitoring timer starts, the monitoring timer is not reset and continues to run.
4. In general, when the monitoring timer has started, it does not reset until it expires. However, as exceptions, it resets in the following cases:
   - When `web-authentication dead-interval 0` is configured by using the `web-authentication radius-server dead-interval` command
   - When information about the Web authentication RADIUS server operating as the current server is deleted by using the `web-authentication radius-server host` configuration command
   - When the `clear radius-server` operation command is executed
5. If the monitoring timer expires while the authentication sequence is being executed on a terminal subject to authentication, restoration of the primary Web authentication RADIUS server is not performed until the executed authentication sequence is completed.

Related commands

aaa authentication web-authentication

web-authentication port

web-authentication system-auth-control

web-authentication radius-server host

web-authentication radius-server host

Configures the RADIUS server used for Web authentication.

Syntax

To set or change information:

web-authentication radius-server host {*<ipv4 address>* | *<ipv6 address>*} [auth-port *<port>*] [acct-port *<port>*] [timeout *<seconds>*] [retransmit *<retries>*] [key *<string>*]

To delete information:

no web-authentication radius-server host {*<ipv4 address>* | *<ipv6 address>*}

Input mode

`(config)`

Parameters

{*<ipv4 address>* | *<ipv6 address>*}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 address of the RADIUS server in colon notation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <ipv4 address>: IPv4 unicast address

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   <ipv6 address>: IPv6 global unicast address

   ::2 to fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff, fec0:: to feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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:

   The period of time set by using the `radius-server timeout` command is

used. If no period is set, the initial value is 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:

   The number of times set by using the `radius-server retransmit` command is used. If no value is set, the initial value is 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 the `radius-server key` command is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Specify with 64 or fewer characters. For details about the characters that can be specified, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The RADIUS server settings registered by using the `radius-server host` command are used.

If the `radius-server host` command is not registered, user authentication is performed by using the internal Web authentication DB without using the RADIUS server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. When this command is set, the setting information of the RADIUS server referenced by Web authentication has priority over the information set by the `radius-server host` command (the settings of the `radius-server host` command are not applied). For details about the settings of the general-use RADIUS server information and the Web authentication RADIUS server information, see the *Configuration Guide Vol. 2*.
4. A maximum of four Web authentication RADIUS servers can be specified for each Switch.
5. `127.*.*.*` cannot be set as an IPv4 address.
6. If the `key` parameter is omitted and the `radius-server key` command is not set, the

RADIUS server is disabled.

7. If multiple Web authentication RADIUS servers are configured, the address displayed first by using the `show radius-server` operation command is the address of the primary Web authentication RADIUS server. The primary Web authentication RADIUS server is used as the first current server (the destination for RADIUS authentication requests during operation).

   If a failure occurred in the primary Web authentication RADIUS server, the current server switches to the next effective Web authentication RADIUS server (secondary RADIUS server). For details about automatic restoration of the primary Web authentication RADIUS server, see the description about the `web-authentication radius-server dead-interval` command.

8. If a RADIUS server with an IP address that matches has already been registered in the general-use RADIUS server configuration, other authentication-specific RADIUS server configuration, or the RADIUS server group configuration, all these parameters are replaced by the new commands that were entered automatically.

Related commands

aaa authentication web-authentication

web-authentication port

web-authentication system-auth-control

web-authentication redirect-mode

Sets a protocol to display the Web authentication Login page when the URL redirect functionality is enabled.

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 }

Sets a protocol to display the Web authentication Login page when the URL redirect functionality is enabled.

- Default value when this parameter is omitted:

  This parameter cannot be omitted.

- Range of values:

  `http`: The Login page for http is displayed.

  `https`: The Login page for https is displayed.

Default behavior

The Login page for https is displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. This command is invalid if the `no web-authentication redirect enable` command is set.

Related commands

web-authentication system-auth-control

web-authentication port

web-authentication redirect enable

web-authentication redirect enable

The `no web-authentication redirect enable` command disables the URL redirect functionality.

Syntax

To set information:

no web-authentication redirect enable

To delete information:

web-authentication redirect enable

Input mode

`(config)`

Parameters

None

Default behavior

The URL redirect functionality is enabled.

Impact on communication

After the `no web-authentication redirect enable` command has been set, the URL redirect functionality does not operate.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication redirect polling

Performs alive monitoring of an external Web server and, if a failure occurs, redirect the user to the Web server of the Switch.

Syntax

To set information:

web-authentication redirect polling tcp [interval *<seconds>*] [dead-count *<count>*] [alive-count *<count>*]

To delete information:

no web-authentication redirect polling

Input mode

`(config)`

Parameters

tcp

Uses tcp packets for monitoring.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

interval *<seconds>*

Sets the monitoring interval.

1. Default value when this parameter is omitted:

   60 (seconds)

2. Range of values:

   10 to 3600 (seconds)

dead-count *<count>*

Sets the number of times a no-response is detected that must occur to determine that a failure has occurred.

1. Default value when this parameter is omitted:

   1 (time)

2. Range of values:

   1 to 5 (times)

alive-count *<count>*

Sets the number of times a response state is detected that must occur to determine that the state is normal.

1. Default value when this parameter is omitted:

   1 (time)

2. Range of values:

   1 to 5 (times)

Default behavior

The user is redirected to the external server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. This command is invalid if the `no web-authentication redirect enable` command is set.
4. If DNS resolution is not working, the monitoring fails.
5. Monitoring via proxy is not supported.

Related commands

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication redirect enable

web-authentication redirect queries

web-authentication redirect target

web-authentication redirect queries

Adds the parameters related to the Switch and terminal to be authenticated to the URL of the redirect destination (external Web server) as queries.

Syntax

To set information:

web-authentication redirect queries [switch-hostname] [switch-mac] [switch-ip] [client-mac] [client-vlan] [client-ip] [port] [original-url]

To delete information:

no web-authentication redirect queries

Input mode

`(config)`

Parameters

[switch-hostname] [switch-mac] [switch-ip] [client-mac] [client-vlan] [client-ip] [port] [original-url]

Select the queries to be added by setting the corresponding parameters. When entering this command, you cannot omit all of the parameters. Set at least one parameter.

switch-hostname

Adds the host name of the Switch (`hostname` command).

switch-mac

Adds the system MAC address of the Switch.

switch-ip

Adds the real IP address of the Switch.

client-mac

Adds the MAC address of the terminal to be authenticated.

client-vlan

Adds the VLAN number of the terminal to be authenticated.

client-ip

Adds the IP address of the terminal to be authenticated.

port

Adds the port to which the terminal to be authenticated is connected.

original-url

Adds the pre-redirect URL.

1. Default value when this parameter is omitted:

   Queries for the omitted parameters are not added..

2. Range of values:

   switch-hostname, switch-mac, switch-ip, client-mac, client-vlan, client-ip, port, and original-url

Default behavior

Queries are not added to the URL when the user is redirected to the external Web server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. This command is invalid if the `no web-authentication redirect enable` command is set.
4. When specifying `original-URL`, for details about the restrictions on the number of characters and character codes for the pre-redirect URL, see *8 Description of Web Authentication* in the *Configuration Guide Vol. 2*.

Related commands

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication redirect enable

web-authentication redirect polling

web-authentication redirect target

web-authentication redirect target

Changes the redirect destination for the URL redirect functionality to the specified external Web server.

Syntax

To set information:

web-authentication redirect target *<url>*

To delete information:

no web-authentication redirect target

Input mode

`(config)`

Parameters

<url>]

Specifies the URL of the external Web server to which the user is to be redirected.

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. For the characters that can be specified, see *Specifiable values for parameters.*

   Enter the value in the following format:

   Format: `"`*<scheme>*`://`*<host>*`[:`*<port>*`][`/*<path>*`][?`*<query>*`]"`

   <scheme>: Enter `http` or `https` in lowercase.

   <host>: Specify the host name or IPv4 address described in *Specifiable values for parameters*.

   <port>: Specify a number in the range from 1 to 65535. This can be omitted.

   <path>: See *Any character string* in *Specifiable values for parameters* (excluding a semicolon (;) and question mark (?)). This can be omitted.

   <query>: See *Any character string* in *Specifiable values for parameters* (excluding a forward slash (/), semicolon (;), and question mark (?)). This can be omitted.

   Example

   (config)# web-authentication redirect target "http://www.example.com:80/login.html?value=3"

Default behavior

The user is redirected to the Web server of the Switch.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. This command is invalid if the `no web-authentication redirect enable` command is set.
4. If the login failed page is displayed due to a password input error or for other reasons and then you click the **login page** button, the login page for the internal Web server of the Switch is displayed.

Related commands

web-authentication system-auth-control

web-authentication port

authentication ip access-group

authentication arp-relay

web-authentication redirect enable

web-authentication redirect polling

web-authentication redirect queries

web-authentication roaming

Sets communication permissions (roaming) when the port for an authenticated terminal changes to another port connected via a hub or similar means without a link-down event occurring.

Syntax

To set or change information:

web-authentication roaming [action trap]

To delete information:

no web-authentication roaming

Input mode

`(config)`

Parameters

[action trap]

When a change to another port due to roaming is detected, a private trap is issued.

- Default value when this parameter is omitted:

  When a change to another port due to roaming is detected, a private trap is not issued.

- Range of values:

  action trap

Default behavior

Changing the port of an authenticated terminal is not permitted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If the destination port is a port in dynamic VLAN mode and the change of port is within the same VLAN, communication is possible after the change.
4. If the DHCP snooping functionality is also used when this command is set and if the port of an authenticated terminal changes to another port, the authentication status also moves to the destination port. However, communication is impossible because the binding database is not updated.
5. When private traps are issued, use the `snmp-server host` command to set the destination IP address for traps and `web-authentication`.

Related commands

web-authentication system-auth-control

web-authentication port

snmp-server host

web-authentication static-vlan roaming

Sets communication permissions (roaming) when the port for an authenticated terminal changes to another port connected via a hub or similar means without a link-down event occurring.

Syntax

To set or change information:

web-authentication static-vlan roaming [action trap]

To delete information:

no web-authentication static-vlan roaming

Input mode

`(config)`

Parameters

[action trap]

When a change to another port due to roaming is detected, a private trap is issued.

- Default value when this parameter is omitted:

  When a change to another port due to roaming is detected, a private trap is not issued.

- Range of values:

  action trap

Default behavior

Communication is not permitted when an authenticated terminal moves to another port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If the destination port is a port in fixed VLAN mode and the move within the same VLAN, communication is possible after the move.
4. If the DHCP snooping functionality is also used when this command is set and if the port of an authenticated terminal changes to another port, the authentication status also moves to the destination port. However, communication is impossible because the binding database is not updated.
5. When private traps are issued, use the `snmp-server host` command to set the destination IP address for traps and `web-authentication`.

Related commands

web-authentication system-auth-control

web-authentication port

snmp-server host

web-authentication system-auth-control

Enables Web authentication.

Note that if the `no web-authentication system-auth-control` command is executed, Web authentication 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` configuration command is executed, authenticated users are logged out.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
2. Even if the `no web-authentication system-auth-control` command is executed, user information registered in the internal Web authentication DB is saved in its current state.

Related commands

None

web-authentication user-group

Enables the user ID-based authentication method.

To handle IDs in the forms `[<User ID>]` and `[<Authentication method list name>]`, use the at mark (`@`) to separate the entered user IDs.

Syntax

To set information:

```
web-authentication user-group
```

To delete information:

```
no web-authentication user-group
```

Input mode

`(config)`

Parameters

None

Default behavior

Entered user IDs are not separated by an at mark (`@`).

Impact on communication

If a change is made, all authentications are canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If at least one of the following commands is set for a Switch, this command cannot be set:
    - dot1x authentication
    - mac-authentication authentication
    - web-authentication authentication
4. If the authentication method list name separated from entered user IDs does not match the authentication method list name set by using the `aaa authentication web-authentication` command, the default settings of the Switch are used.

Related commands

aaa authentication web-authentication

web-authentication system-auth-control

web-authentication port

web-authentication user replacement

Enables the switch-user option.

Enables authentication with a different user ID after successful authentication with the first user ID when several user IDs are used for a terminal.

Syntax

To set information:

```
web-authentication user replacement
```

To delete information:

```
no web-authentication user replacement
```

Input mode

`(config)`

Parameters

None

Default behavior

Login from an authenticated terminal by using another user name is not permitted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. If authentication is canceled when the user has been switched, it is not possible to return to the first user.

Related commands

web-authentication system-auth-control

web-authentication web-port

When the URL redirect functionality is enabled, this command sets an additional TCP destination port number for a frame subject to URL redirect on a Switch.

Usually, one port number each can be added to the port number assigned for http (80) and for https (443).

Syntax

To set or change information:

web-authentication web-port {http *<port>* | https *<port>*}

To delete information:

no web-authentication web-port {http | https}

Input mode

`(config)`

Parameters

{http *<port>* | https *<port>*}

Specify the port number to be used for http protocol or https protocol communication. Note that if OAN is also used, port numbers 832 and 9698 are used by OAN.

- Default value when this parameter is omitted:

  This parameter cannot be omitted.

- Range of values:

  For the http parameter: 1 to 65535 (except 443)

  For the https parameter: 1 to 65535 (except 80)

Default behavior

Frames with the following initial port number are subject to URL redirection.

- http: 80
- https: 443

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All Web authentication settings take effect when the `web-authentication system-auth-control` command is set.
2. See *Table 25-1 Configuration commands and Web authentication modes* for the authentication mode in which the command's settings are operable.
3. The number of TCP destination port numbers that can be set by using this command is one each for the http and https parameters.

Related commands

authentication ip access-group

web-authentication web-port

authentication arp-relay

web-authentication port

web-authentication system-auth-control

26. MAC-based Authentication

Correspondence between configuration commands and authentication modes

The following table describes MAC-based authentication modes in which MAC-based authentication configuration commands can be set.

Table 26-1 Configuration commands and MAC-based authentication modes

Command name	MAC-based authentication modes[#3]	
	Fixed VLAN Mode	**Dynamic VLAN Mode**
aaa accounting mac-authentication	Y	Y
aaa authentication mac-authentication	Y	Y
aaa authentication mac-authentication end-by-reject	Y	Y
authentication arp-relay[#1]	Y	Y
authentication ip access-group[#1]	Y	Y
mac-authentication access-group	Y	Y
mac-authentication authentication	Y	Y
mac-authentication auto-logout	Y	Y
mac-authentication id-format	Y	Y
mac-authentication logging enable	Y	Y
mac-authentication max-timer	Y	Y
mac-authentication password	Y	Y
mac-authentication port[#2]	Y	Y
mac-authentication radius-server dead-interval	Y	Y
mac-authentication radius-server host	Y	Y
mac-authentication roaming	--	Y
mac-authentication static-vlan roaming	Y	--
mac-authentication system-auth-control	Y	Y
mac-authentication timeout quiet-period	Y	Y
mac-authentication timeout reauth-period	Y	Y

Command name	MAC-based authentication modes#3	
	Fixed VLAN Mode	Dynamic VLAN Mode
mac-authentication vlan-check	Y	--

Legend

Y: The command operates according to the settings.

--: The command can be entered, but it will have no effect.

N: The command cannot be entered.

#1

For details about command input formats, see *23. Common to Layer 2 Authentication*.

#2

The specification of this command affects the switching of authentication modes.

#3

For details such as a description of the authentication modes, see the *Configuration Guide Vol. 2*.

aaa accounting mac-authentication

Sends accounting information for MAC-based authentication to an accounting server.

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

default

Sets the default accounting method of a Switch.

start-stop

If authentication is canceled, the stop accounting notification is sent to the accounting server.

group radius

The RADIUS server is used as the accounting server.

Default behavior

A notification is not sent to the accounting server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

aaa authentication mac-authentication

mac-authentication system-auth-control

radius-server host or mac-authentication radius-server host

aaa authentication mac-authentication

Sets an authentication method group for MAC-based authentication.

If the first specified method fails, the second specified method is used. If authentication fails, you can change the authentication method by using the `aaa authentication mac-authentication end-by-reject` command.

If `default` is set, one entry can be set. If an authentication method list name is specified, a maximum of four entries can be set.

Syntax

To set or change information:

aaa authentication mac-authentication default *<Method>* [*<Method>*]

aaa authentication mac-authentication *<List name>* group *<Group name>*

To delete information:

no aaa authentication mac-authentication {default | *<List name>*}

Input mode

`(config)`

Parameters

default *<Method>* [*<Method>*]

Sets the default authentication method of a Switch. You cannot specify the same *<Method>* more than once.

For *<Method>*, specify `group radius` or `local`.

group radius

MAC-based authentication is performed by a RADIUS server. The RADIUS server to use is a MAC-based authentication RADIUS server or a general-use RADIUS server.

local

Local authentication is performed. The internal MAC-based authentication DB is used.

<List name>

Sets the name of an authentication method list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

   We recommend that you use an upper-case letter for the first character.

   However, you cannot use the following character strings:

   - At mark (`@`)
   - `default` or a character string beginning with `default`
   - `end-by-reject` or a character string beginning with `end-by-reject`

group *<Group name>*

MAC-based authentication is performed by a RADIUS server. The RADIUS server to use is a RADIUS server group. Specify the group name set by the `aaa group server` `radius` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

Authentication is performed by using the internal MAC-based authentication DB instead of using the RADIUS server.

Impact on communication

When you change the Switch default, the Switch clears the authentication status of the terminals authenticated with the authentication method of the Switch default.

When you change the setting of the authentication method list, the Switch clears the authentication status of the terminals authenticated with the corresponding authentication method list.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. Enabling of this command requires a separate authentication setting for the RADIUS server.
4. The forced authentication functionality for MAC-based authentication operates only when RADIUS authentication is set. If multiple authentication methods are set, the forced authentication functionality does not operate.

Related commands

aaa authentication mac-authentication end-by-reject

aaa group server radius

mac-authentication system-auth-control

mac-authentication authentication

radius-server host or mac-authentication radius-server host

aaa authentication mac-authentication end-by-reject

Terminates authentication if authentication is denied. If the authentication fails due to communication abnormality, such as an unresponsive RADIUS server, the next authentication method specified by the `aaa authentication mac-authentication` command is used to perform authentication.

Syntax

To set information:

aaa authentication mac-authentication end-by-reject

To delete information:

no aaa authentication mac-authentication end-by-reject

Input mode

`(config)`

Parameters

None

Default behavior

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

Impact on communication

Authentication of terminals authenticated by the MAC-based authentication functionality is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
2. This command is only valid for authentication methods specified by the `aaa authentication mac-authentication` command.

Related commands

aaa authentication mac-authentication

mac-authentication access-group

By applying the MAC access list to MAC-based authentication ports, sets whether terminals are to be authenticated or not by using MAC addresses.

Syntax

To set or change information:

mac-authentication access-group *<access list name>*

To delete information:

no mac-authentication access-group

Input mode

`(config)`

Parameters

<access list name>

Specifies the identifier of the MAC access list that is to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

All terminals connected to MAC-based authentication ports are subject to authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. Implicit discard is present in a registered MAC access list. If the MAC address of a terminal is not found in the MAC access list you have set, the terminal is not subject to authentication due to implicit discard.
4. If a non-existent MAC access list is set, no operation is performed. The identifier of the MAC access list is registered.

Related commands

mac-authentication system-auth-control

mac access-list extended

mac-authentication authentication

Sets the name of an authentication method list for the port-based authentication method.

Syntax

To set or change information:

mac-authentication authentication *<List name>*

To delete information:

no mac-authentication authentication

Input mode

`(config-if)`

Parameters

<List name>

Sets the authentication method list name set by using the `aaa authentication mac-authentication` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that has no more than 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters* (with the exception of the at mark (`@`)).

   We recommend that you use an upper-case letter for the first character.

Default behavior

MAC-based authentication is performed by using the default values of the Switch.

Impact on communication

Authentication of a terminal for a port whose authentication method list name has been changed is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. This command cannot be set when the `web-authentication user-group` command has been set.
4. If the authentication method list name set by using this command does not match the authentication method list name set by using the `aaa authentication mac-authentication` command, the default settings of the Switch are used.

Related commands

aaa authentication mac-authentication

mac-authentication authentication

mac-authentication system-auth-control

mac-authentication port

mac-authentication auto-logout

The `no mac-authentication auto-logout` command disables automatic cancellation of authentication if no frames are received from a terminal authenticated by MAC-based authentication for a certain period of time.

Syntax

To set information:

no mac-authentication auto-logout

To change information:

mac-authentication auto-logout delay-time <*Seconds*>

To delete information:

mac-authentication auto-logout

Input mode

`(config)`

Parameters

delay-time <*Seconds*>

MAC-based authentication entries registered in the MAC address table after authentication are subject to the delay time.

If no frames have been received from a terminal after the period of time set by using this command (non-communication monitoring time) elapses, the applicable MAC-based authentication entries are deleted from the MAC table and authentication is canceled.

If 0 is set, the default value (3600 seconds) is used as the non-communication monitoring time.

1. Default value when this parameter is omitted:

   3600 seconds is used as the non-communication monitoring time for the MAC-based authentication entries registered after authentication.

2. Range of values:

   0, 60 to 86400 (seconds)

Default behavior

After authentication, if no frames are received from a terminal for the applicable MAC-based authentication entry when 3600 seconds has passed, the applicable MAC-based authentication entry is deleted from the MAC table automatically and authentication is canceled.

Impact on communication

After the `no mac-authentication auto-logout` command is set, authentication is not automatically canceled even if a terminal authenticated using MAC-based authentication detects that forwarding has not been performed on the terminal for a certain period of time.

If `mac-authentication auto-logout delay-time` is set, the terminal operates according to the time that has been set.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. The non-communication monitoring time on an authenticated terminal in fixed VLAN mode or dynamic VLAN mode takes effect if the following condition exists:
    - The MAC-based authentication fixed VLAN mode or dynamic VLAN mode is in effect and `mac-authentication auto-logout` is enabled.

Related commands

mac-authentication system-auth-control

mac-authentication port

mac-address-table aging-time

mac-authentication id-format

When using RADIUS authentication, specifies MAC address format for authentication requests to the RADIUS server.

Syntax

To set or change information:

mac-authentication id-format *<Type>* [capitals]

To delete information:

no mac-authentication id-format

Input mode

`(config)`

Parameters

<Type>

Sets MAC address format used when an authentication request is sent to the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 3

   0: *xx*-*xx*-*xx*-*xx*-*xx*-*xx*

   1: *xxxxxxxxxxxx*

   2: *xxxx*.*xxxx*.*xxxx*

   3: *xx*:*xx*:*xx*:*xx*:*xx*:*xx*

capitals

Use this parameter to set a MAC address used when an authentication request is sent to the RADIUS server in hexadecimal uppercase format.

1. Default value when this parameter is omitted:

   Lowercase characters are used.

2. Range of values:

   capitals

Default behavior

Authentication requests are sent to the RADIUS server in hexadecimal lowercase character format, such as `Type 0 (`*`xx-xx-xx-xx-xx-xx`*`)`.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication`

`system-auth-control` command is set.

2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

mac-authentication system-auth-control

aaa authentication mac-authentication

mac-authentication logging enable

Enables the output of operation log information for MAC-based authentication to a syslog server.

Syntax

To set information:

mac-authentication logging enable

To delete information:

no mac-authentication logging enable

Input mode

`(config)`

Parameters

None

Default behavior

Operation log information is not output to a syslog server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

mac-authentication system-auth-control

logging event-kind

mac-authentication max-timer

Sets the maximum connection time.

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 time (in minutes) an authenticated terminal is allowed to be connected. After a successful authentication, if the period of time set by using this command elapses, the authentication is canceled automatically.

If `infinity` is specified, there is no limit to the connection time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 1440 (minutes) or `infinity`

Default behavior

Authentication is not canceled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. If the value for the maximum connection time is decreased or increased, the previous setting is applied to terminal that is currently authenticated, and the setting values take effect only from the next login.
4. The connection time for MAC-based authentication does not use the time of a Switch. Accordingly, if the date and time is changed by using the `set clock` operation command, the connection time is not affected.

Related commands

mac-authentication system-auth-control

mac-authentication password

When the RADIUS authentication method is used, this command sets the password used for sending authentication requests 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 password used when sending authentication requests to the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The password can be 1 to 32 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

When the `mac-authentication id-format` command is set, the MAC address of the terminal subject to authentication in the format set by using that command becomes the password.

If the `mac-authentication id-format` command is not set, the MAC address of a terminal subject to authentication in *xx-xx-xx-xx-xx-xx* format (a to f must be lowercase) becomes the password.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. The passwords set by using this command are common to all MAC-based authentication RADIUS authentication terminals.

Related commands

mac-authentication system-auth-control

mac-authentication password

mac-authentication id-format

aaa authentication mac-authentication

mac-authentication port

Sets the authentication mode for ports.

Syntax

To set information:

```
mac-authentication port
```

To delete information:

```
no mac-authentication port
```

Input mode

`(config-if)`

Parameters

None

Default behavior

Mac-based authentication is not performed in this 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

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

mac-authentication system-auth-control

authentication ip access-group

authentication arp-relay

mac-authentication radius-server dead-interval

Configures the timer for monitoring automatic restoration to the primary MAC-based authentication RADIUS server from the MAC-based authentication RADIUS server.

The primary MAC-based authentication RADIUS server is restored when either of the following occurs: The current server (the destination for RADIUS authentication requests in operation) switches to a valid secondary MAC-based authentication RADIUS server, or when all servers are disabled, the monitoring timer starts, and the period of time set by this command elapses (when the monitoring timer expires).

Syntax

To set or change information:

mac-authentication radius-server dead-interval *<Minutes>*

To delete information:

no mac-authentication radius-server dead-interval

Input mode

`(config)`

Parameters

<Minutes>

Configures the timer for monitoring automatic restoration to the primary MAC-based authentication RADIUS server from the secondary MAC-based authentication RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 1440 (minutes)

   If 0 is set, RADIUS authentication requests are always initiated from the primary MAC-based authentication RADIUS server.

Default behavior

The primary MAC-based authentication RADIUS server is automatically restored 10 minutes after the current server switches to the secondary MAC-based authentication RADIUS server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

1. If the secondary MAC-based authentication RADIUS server is operating as the current server, and if the value of the monitoring timer is changed, the progress to that time is used as the judgment value and the result is applied.
2. If this command configuration is deleted after the monitoring timer starts, the monitoring timer counter continues without being reset and runs for 10 minutes (default value).

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. If three or more MAC-based authentication RADIUS servers are configured and another MAC-based authentication RADIUS server becomes the current server after the monitoring timer starts, the monitoring timer is not reset and continues to run.
4. In general, when the monitoring timer has started, it does not reset until it expires. However, as exceptions, it resets in the following cases:
   - When `mac-authentication dead-interval 0` is configured by using the `mac-authentication radius-server dead-interval` command
   - When information about the MAC-based authentication RADIUS server operating as the current server is deleted by using the `mac-authentication radius-server host` configuration command
   - When the `clear radius-server` operation command is executed
5. If the monitoring timer expires while the authentication sequence is being executed on a terminal subject to authentication, restoration of the primary MAC-based authentication RADIUS server is not performed until the executed authentication sequence is completed.

Related commands

aaa authentication mac-authentication

mac-authentication port

mac-authentication system-auth-control

mac-authentication radius-server host

mac-authentication radius-server host

Configures the RADIUS server used for MAC-based authentication.

Syntax

To set or change information:

mac-authentication radius-server host {*<ipv4 address>* | *<ipv6 address>*} [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>*}

Input mode

`(config)`

Parameters

{*<ipv4 address>* | *<ipv6 address>*}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 address of the RADIUS server in colon notation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <ipv4 address>: IPv4 unicast address

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   <ipv6 address>: IPv6 global unicast address

   ::2 to fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff, fec0:: to feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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:

   The period of time set by using the `radius-server timeout` command is

used. If no period is set, the initial value is 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:

   The number of times set by using the `radius-server retransmit` command is used. If no value is set, the initial value is 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 the `radius-server key` command is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Specify a character string that has no more than 64 characters. For details about the characters that can be specified, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The RADIUS server settings registered by using the `radius-server host` command are used.

If the `radius-server host` command is not registered, user authentication is performed by using the internal MAC-based authentication DB without using the RADIUS server.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. When this command is set, 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 (the settings of the `radius-server host` command are not applied). For details about settings for the general-use RADIUS server information and the MAC-based authentication RADIUS server information, see the *Configuration Guide Vol. 2*.
4. A maximum of 4 MAC-based authentication RADIUS servers can be specified for each Switch.

5. `127.*.*.*` cannot be set as an IPv4 address.
6. If the `key` parameter is omitted and the `radius-server key` command is not set, the RADIUS server is disabled.
7. If multiple MAC-based authentication RADIUS servers are configured, the address displayed first by using the `show radius-server` operation command is the primary MAC-based authentication RADIUS server. The primary MAC-based authentication RADIUS server is used as the first current server (the destination for RADIUS authentication requests during operation).

   If a failure occurs on the primary MAC-based authentication RADIUS server, the current server switches to the next effective MAC-based authentication RADIUS server (secondary RADIUS server). For details about automatic restoration of the primary MAC-based authentication RADIUS server, see the description for the `mac-authentication radius-server dead-interval` command.
8. If a RADIUS server with an IP address that matches has already been registered in the general-use RADIUS server configuration, some other authentication-specific RADIUS server configuration, or the RADIUS server group configuration, all these parameters are replaced by the new commands that were entered automatically.

Related commands

aaa authentication mac-authentication

mac-authentication port

mac-authentication system-auth-control

mac-authentication roaming

Sets communication permissions (roaming) when the port for an authenticated terminal changes to another port connected via a hub or similar means without a link-down event occurring.

Syntax

To set or change information:

mac-authentication roaming [action trap]

To delete information:

no mac-authentication roaming

Input mode

`(config)`

Parameters

[action trap]

When a change to another port due to roaming is detected, a private trap is issued.

- Default value when this parameter is omitted:

  When a change to another port due to roaming is detected, a private trap is not issued.

- Range of values:

  action trap

Default behavior

Communication is not permitted when an authenticated terminal moves to another port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. If the destination port is a port in dynamic VLAN mode and the change of port is within the same VLAN, communication is possible after the change.
4. If the DHCP snooping functionality is also used when this command is set and if the port of an authenticated terminal changes to another port, the authentication status also moves to the destination port. However, communication is impossible because the binding database is not updated.
5. Before issuing private traps, you must use the `snmp-server host` command to set the destination IP address for traps and `mac-authentication`.

mac-authentication roaming

Related commands

mac-authentication system-auth-control

mac-authentication port

snmp-server host

mac-authentication static-vlan roaming

Sets communication permissions (roaming) when the port for an authenticated terminal changes to another port connected via a hub or similar means without a link-down event occurring.

Syntax

To set or change information:

mac-authentication static-vlan roaming [action trap]

To delete information:

no mac-authentication static-vlan roaming

Input mode

`(config)`

Parameters

[action trap]

When a change to another port due to roaming is detected, a private trap is issued.

- Default value when this parameter is omitted:

  When a change to another port due to roaming is detected, a private trap is not issued.

- Range of values:

  action trap

Default behavior

Communication is not permitted when an authenticated terminal moves to another port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. If the destination port is a port in fixed VLAN mode and the move within the same VLAN, communication is possible after the move.
4. If the DHCP snooping functionality is also used when this command is set and if the port of an authenticated terminal changes to another port, the authentication status also moves to the destination port. However, communication is impossible because the binding database is not updated.
5. Before issuing private traps, you must use the `snmp-server host` command to set the destination IP address for traps and `mac-authentication`.

```
mac-authentication static-vlan roaming
```

Related commands

mac-authentication system-auth-control

mac-authentication port

snmp-server host

mac-authentication system-auth-control

Enables MAC-based authentication.

Note that if the `no mac-authentication system-auth-control` command is executed, MAC-based authentication 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 `no mac-authentication system-auth-control` is executed, the authentication of the authenticated terminals is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
2. If `no mac-authentication system-auth-control` is executed, terminal information registered in the internal MAC-based authentication DB is saved in its current state.

Related commands

None

mac-authentication timeout quiet-period

Sets the time during which re-authentication will not be attempted (re-authentication delay timer) for the same terminal (MAC address) when authentication fails. No authentication processing is performed during this period.

Syntax

To set or change information:

mac-authentication timeout quiet-period *<Seconds>*

To delete information:

no mac-authentication timeout quiet-period

Input mode

`(config)`

Parameters

<Seconds>

Specifies the re-authentication delay timer in seconds. If you want to restart authentication processing immediately after authentication fails, set 0.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0, 60 to 86400 (seconds)

Default behavior

No authentication processing for the same terminal is performed for 300 seconds after MAC-based authentication failure.

Impact on communication

None

When the change is applied

1. When authentication fails
2. When the re-authentication delay timer that is running times out and the value of the timer becomes 0.
3. When the `clear mac-authentication auth-state` operation command is executed to cancel the authentication of specific terminals or the authentication of all authenticated terminals for an entire Switch.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.
3. When multistep authentication is used, a value other than 0 must be set for this command.

Related commands

mac-authentication system-auth-control

mac-authentication timeout reauth-period

Sets the interval for re-authenticating terminals after an authentication has been successful.

Syntax

To set or change information:

mac-authentication timeout reauth-period *<Seconds>*

To delete information:

no mac-authentication timeout reauth-period

Input mode

`(config)`

Parameters

<Seconds>

Specifies the interval (in seconds) for re-authenticating a terminal. If 0 is set, re-authentication is not performed and operation continues.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0, 600 to 86400 (seconds)

Default behavior

3600 seconds is used as the interval for re-authenticating a terminal.

Impact on communication

None

When the change is applied

- When the interval for re-authenticating the current terminals times out, and the value of the timer becomes 0.
- When the `clear mac-authentication auth-state` operation command is executed to cancel the authentication of specific terminals or the authentication of all authenticated terminals for an entire Switch.
- When the authentication of a terminal succeeds when no authenticated terminals exist

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.

Related commands

mac-authentication system-auth-control

mac-authentication vlan-check

Checks the VLAN ID when checking a MAC address during authentication processing.

For the RADIUS authentication method, the MAC address string, the string set by using this command (`%VLAN` is set by default), and the VLAN ID are combined and used as the user ID for sending an authentication request to the RADIUS server.

For the local authentication method, the MAC address string and the VLAN ID are checked against the internal MAC-based authentication DB (If there is no VLAN ID information in the internal MAC-based authentication DB, only the MAC address string is used for the check).

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>*

This parameter applies only to the RADIUS authentication method.

The parameter sets a character string that is added to the user ID when an authentication request is sent to the RADIUS server.

This parameter is invalid for the local authentication method.

1. Default value when this parameter is omitted:

   `%VLAN` is set.

2. Range of values:

   1 to 64 characters can be set. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

No VLAN IDs are added during the MAC-based authentication check.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All MAC-based authentication settings take effect when the `mac-authentication system-auth-control` command is set.
2. See *Table 26-1 Configuration commands and MAC-based authentication modes* for the authentication mode in which the command's settings are operable.

```
mac-authentication vlan-check
```

Related commands

mac-authentication system-auth-control

mac-authentication port

aaa authentication mac-authentication

27. Multistep Authentication

authentication multi-step

authentication multi-step

Configures a multistep authentication port.

Syntax

To set or change information:

```
authentication multi-step  [{permissive | dot1x}]
```

To delete information:

```
no authentication multi-step
```

Input mode

`(config-if)`

Parameters

{permissive | dot1x}

permissive

Permits both Web authentication and IEEE 802.1X authentication for a terminal on which the first step (MAC-based authentication) has failed.

1. Default value when this parameter is omitted:

   For a terminal on which the first step (MAC-based authentication) has failed, neither Web authentication nor IEEE 802.1X authentication is permitted.

dot1x

Permits MAC-based authentication and IEEE 802.1X authentication as the first step of authentication. For a terminal on which the first step (MAC-based authentication or IEEE 802.1X authentication) has failed, Web authentication is not permitted.

1. Default value when this parameter is omitted:

   For a terminal on which the first step (MAC-based authentication) has failed, neither Web authentication nor IEEE 802.1X authentication is permitted.

2. Range of values:

   `permissive` or `dot1x`

Default behavior

The port operates as a single authentication port.

Impact on communication

The authenticated state of a terminal connected to the applicable port is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

28. Secure Wake-on-LAN [OS-L2A]

http-server [OS-L2A]

Enables the HTTP server functionality.

Syntax

To set information:

http-server

To delete information:

no http-server

Input mode

`(config)`

Parameters

None

Default behavior

When the `web-authentication system-auth-control` command is set: Enabled

When the `web-authentication system-auth-control` command is not set: Disabled

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, display of the Secure Wake-on-LAN user authentication page and Web authentication Login page can be enabled.
2. When the `web-authentication system-auth-control` command has been set, display of the Secure Wake-on-LAN user authentication screen and Web authentication Login page can be enabled.
3. When the `web-authentication system-auth-control` command has been set, operation of the Web authentication functionality is also enabled. Therefore, when using the Secure Wake-on-LAN user authentication screen only, set the `http-server` command.
4. If both this command and the `web-authentication system-auth-control` command have been set, operation of the Secure Wake-on-LAN functionality is not affected. The following table explains the combinations of command settings.

Configuration settings		Secure Wake-on-LAN		Web authentication	
http-server	**web-authentication system-auth-control**	**User authentication page**	**Functionality**	**Login page**	**Functionality**
Not set	Not set	Not displayed.	Does not operate.	Not displayed.	Does not operate.
	Set	Can be displayed.	Operates.	Can be displayed.	Operates.
Set	Not set	Can be displayed.	Operates.	Can be displayed.	Does not operate.
	Set	Can be displayed.	Operates.	Can be displayed.	Operates.

Related commands

None

Part 10: Security

29. DHCP Snooping

ip arp inspection limit rate

Sets the ARP packet reception rate (the number of ARP packets that can be received per second) on the applicable port when the DHCP snooping functionality is enabled on a Switch. ARP packets in excess of this reception rate are discarded.

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-if)`

Parameters

<Packet/s>

Specify 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:

   1 to 300 (packets/s)

Default behavior

The reception rate has no limit.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the `ip arp inspection trust` command is set on the port where the `ip arp inspection limit rate` command is set, the settings of the `ip arp inspection limit rate` command become invalid. As a result, there is no limit on the reception rate for ARP packets.
2. Values specified by using this command set the upper limit for the number of received packets, but do not guarantee operation with the specified value.

Related commands

ip dhcp snooping

ip arp inspection trust

Sets the applicable interface as a trusted port where no dynamic ARP inspection is performed when the DHCP snooping functionality is enabled on a Switch.

Syntax

To set information:

ip arp inspection trust

To delete information:

no ip arp inspection trust

Input mode

```
(config-if)
```

Parameters

None

Default behavior

Dynamic ARP inspection is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. On an interface on which this command is set, even if the interface is accommodated in the VLAN where the dynamic ARP inspection functionality is enabled, the inspection is not performed.
2. The ARP packet reception rate of the interface on which this command is set has no limit.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip arp inspection validate

Sets inspection items to be added to improve the accuracy of the dynamic ARP inspection when the dynamic ARP inspection functionality is enabled on a Switch.

Syntax

To set or change information:

ip arp inspection validate [src-mac] [dst-mac] [ip]

To delete information:

no ip arp inspection validate

Input mode

`(config)`

Parameters

src-mac

This inspection item checks if the source MAC address and the sender MAC address of received ARP packets are the same. This inspection is performed on both an ARP request and an ARP reply.

1. Default value when this parameter is omitted:

   The inspection that checks if the source MAC address and the sender MAC address of the received ARP packet are the same is not performed.

2. Range of values:

   None

dst-mac

This inspection item checks if the destination MAC address and the target MAC address of the received ARP packets are the same. This inspection is performed on an ARP reply.

1. Default value when this parameter is omitted:

   The inspection for checking if the destination MAC address and the target MAC address of the received ARP packet are the same is not performed.

2. Range of values:

   None

ip

This inspection item checks if the target IP address 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.

1. Default value when this parameter is omitted:

   The target IP address of the received ARP packet is not checked.

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 cannot omit all of the parameters in this command. You must set at least one.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip arp inspection vlan

ip arp inspection vlan

Sets the VLAN used for dynamic ARP inspection when the DHCP snooping functionality is enabled on a Switch.

Syntax

To set or 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 inspection.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

add *<VLAN ID list>*

Adds the IDs of VLANs that will be used for the dynamic ARP inspection to the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

remove *<VLAN ID list>*

Removes the IDs of the VLANs used for dynamic ARP inspection from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

Default behavior

The dynamic ARP inspection functionality is not used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set a VLAN ID set by using the `ip dhcp snooping vlan` command.
2. If this command is set, the binding database entries registered by using the `ip source binding` command are also subject to dynamic ARP inspection.
3. If a VLAN set by this command is accommodated on a port set by using the `ip arp inspection trust` command, dynamic ARP inspection is not performed.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping

Enables the DHCP snooping functionality on a Switch.

Syntax

To set information:

```
ip dhcp snooping
```

To delete information:

```
no ip dhcp snooping
```

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

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

The database is saved to internal flash memory.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   flash

mc *<File name>*

The database is saved to a memory card.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <File name>: A maximum of 64 characters can be set.

   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.

   For details about the characters that can be specified, see *Specifiable values for parameters*.

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 wait-to-write 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.
   - A dynamic binding database is registered, updated, or deleted.
   - The `ip dhcp snooping database url` command is set (this includes changes

to the save destination).

- The clear ip dhcp snooping binding operation command is executed

If the Switch power is turned off before the timer expires, the binding database cannot be saved.

2. If the no ip dhcp snooping database url command is entered after the timer set by using the ip dhcp snooping database write-delay command has started, the binding database is not saved.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping database write-delay

Sets the wait-to-write time used 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 wait-to-write time used 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

When `ip dhcp snooping database url` is set, 1800 (seconds) is used.

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 wait-to-write 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.

   - A dynamic binding database is registered, updated, or deleted.
   - The `ip dhcp snooping database url` command is set (this includes changes to the save destination).
   - The `clear ip dhcp snooping binding` operation command is executed

   If the Switch power is turned off before the timer expires, the binding database cannot be saved.

2. If the `no ip dhcp snooping database url` command is entered after the timer set by using the `ip dhcp snooping database write-delay` command has started, the binding database is not saved.

Related commands

ip dhcp snooping

ip dhcp snooping database url

ip dhcp snooping vlan

ip dhcp snooping information option allow-untrusted

Sets this command to allow DHCP packets that have option [82] information to be received on an untrusted port. If this setting is omitted, DHCP packets that have option [82] information are discarded.

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

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 dhcp snooping

ip dhcp snooping limit rate

Sets the DHCP packet reception rate (the number of DHCP packets that can be received per second) on the applicable port. DHCP packets exceeding the reception rate are discarded.

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-if)
```

Parameters

<Packet/s>

Specify the number of DHCP packets that can be received per second.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 300 (packets/s)

Default behavior

The reception rate has no limit.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the `ip dhcp snooping trust` command is set on the port where the `ip dhcp snooping limit rate` command is set, the settings of the `ip dhcp snooping limit rate` command become invalid. As a result, there is no limit on the reception rate for DHCP packets.
2. Values specified by using this command set the upper limit for the number of received packets, but do not guarantee operation with the specified value.

Related commands

ip dhcp snooping

ip dhcp snooping trust

Sets whether the interface is a trusted port or an untrusted port.

Syntax

To set information:

ip dhcp snooping trust

To delete information:

no ip dhcp snooping trust

Input mode

```
(config-if)
```

Parameters

None

Default behavior

The applicable interface operates as an untrusted port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. On an interface on which this command is set, even 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

If this command is not set, the DHCP relay agent cannot be connected to an untrusted port because the MAC address is checked. (If packets are received via a DHCP relay agent, the sender MAC address is 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. A maximum of 64 VLANs can be set with this command.

Syntax

To set or change information:

```
ip dhcp snooping vlan <VLAN ID list>
```

To delete information:

```
no ip dhcp snooping vlan <VLAN ID list>
```

Input mode

`(config)`

Parameters

<VLAN ID list>

Specify the IDs of VLANs on which DHCP snooping is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   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

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 static for the binding database.

Syntax

To set information:

ip source binding *<MAC>* vlan *<VLAN ID>* *<IP address>* interface { gigabitethernet *<IF#>* |tengigabitethernet *<IF#>* | port-channel *<Channel group#>* }

To delete information:

no ip source binding *<MAC>* vlan *<VLAN ID>* *<IP address>* interface { gigabitethernet *<IF#>* |tengigabitethernet *<IF#>* | port-channel *<Channel group#>* }

Input mode

`(config)`

Parameters

<MAC>

Sets the MAC address of a terminal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to ffff.ffff.ffff

<VLAN ID>

Sets the ID of a VLAN to which the terminal is connected.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

<IP address>

Sets the IP address of the terminal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

interface { gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>* }

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:

   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

A maximum of 128 entries can be set. Note, however, that no entries can be set when the number of binding database entries, including dynamic entries, exceeds the maximum number of entries.

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip verify source

Sets this command to use the terminal filter based on the DHCP snooping binding database. (The terminal filter is functionality used to filter the packets of unregistered source IP and MAC addresses.)

Syntax

To set or change information:

```
ip verify source [ { port-security | mac-only } ]
```

To delete information:

```
no ip verify source
```

Input mode

```
(config-if)
```

Parameters

{ port-security | mac-only }

Sets a terminal filter condition.

port-security

Applies the terminal filter to both the source IP and the source MAC addresses.

mac-only

Applies the terminal filter only to source MAC addresses.

1. Default value when this parameter is omitted:

   The terminal filter is applied only to source IP addresses.

2. Range of values:

   None

Default behavior

None

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. The terminal filter functionality is disabled on trusted ports even if this command is set.
2. If this command is set when DHCP snooping is enabled, the terminal filter functionality is enabled even in a VLAN for which DHCP snooping is not valid.
3. If the terminal filter is applied, packets from the terminals that are not registered in the binding database are discarded regardless of the VLAN.

ip verify source

Related commands

ip dhcp snooping

ip dhcp snooping vlan

ip dhcp snooping trust

ip source binding

Part 11: High Reliability Based on Redundant Configurations

30. Power Supply Redundancy

power redundancy-mode

power redundancy-mode

Sets whether to display a message notifying that the redundant power supply has not been implemented.

Syntax

To set information:

```
power redundancy-mode redundancy-check
```

To delete information:

```
no power redundancy-mode
```

Input mode

`(config)`

Parameters

redundancy-check

Checks whether the redundant power supply has been implemented.

If the redundant power supply has not been implemented, the Switch displays a message notifying that the redundant power supply has not been implemented.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The Switch does not check whether the redundant power supply has been implemented.

Even if the redundant power supply has not been implemented, the Switch does not display a message notifying that the redundant power supply has not been implemented.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

31. Uplink Redundancy

switchport backup interface
switchport backup flush-request transmit
switchport backup mac-address-table update exclude-vlan
switchport backup mac-address-table update retransmit
switchport backup mac-address-table update transmit
switchport-backup startup-active-port-selection

switchport backup interface

Specifies the primary or secondary port, and an automatic switch-back time or a timer-based switch-back time.

Syntax

To set or change information:

switchport backup interface {gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*} [preemption-delay *<Seconds>*]

To delete information:

no switchport backup interface

Input mode

`(config-if)`

Parameters

{gigabitethernet *<IF#>* | tengigabitethernet *<IF#>* | port-channel *<Channel group#>*}

Sets the secondary port. The port on which this command is set will be the primary port. Specifiable interfaces are Ethernet and port channel.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <IF#>: See *Specifiable values for parameters*.

   <Channel group#>: See *Specifiable values for parameters*.

preemption-delay *<Seconds>*

Sets an automatic switch-back time or a timer-based switch-back time.

Setting the time enables automatic or timer-based switch-backs.

1. Default value when this parameter is omitted:

   A manual switch-back is performed by using the `set switchport backup interface` operation command.

2. Range of values:

   0 (seconds): Automatic switch-back

   1 to 300 (seconds): Timer-based switch-back

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. When the Spanning Tree Protocol is used at the upstream switch, the status will be `listening` or `learning` after recovering from the link-down state. Communication

cannot be restored immediately. In this case, we recommend that you set the timer-based switch-back time to 30 seconds or longer.

Related commands

None

switchport backup flush-request transmit

Enables the sending of flush control frames to request that the upstream switches clear their MAC address tables.

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)`

Parameters

vlan *<VLAN ID>*

Sets the VLAN Tag value to be added to flush control frames.

1. Default value when this parameter is omitted:

   Flush control frames are sent in the form of untagged frames.

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. If a VLAN Tag value is set here, the flush control frames are sent in the form of tagged frames even if the target port is an access port.
2. Set this command for the primary port.

Related commands

switchport backup interface

switchport backup mac-address-table update exclude-vlan

Sets the VLAN to be excluded when sending MAC address update frames.

Syntax

To set or change information:

switchport backup mac-address-table update exclude-vlan *<VLAN ID list>*

To delete information:

no switchport backup mac-address-table update exclude-vlan

Input mode

`(config-if)`

Parameters

<VLAN ID list>

Sets the list of VLANs to be excluded when MAC address update frames are sent.

Entering a new value overwrites the existing information.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set *<VLAN ID list>* and the specifiable values, see *Specifiable values for parameters*.

Default behavior

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.

Notes

1. You can set a maximum of 200 parameter values for excluding VLANs.

   Example when four VLAN parameter values are set:

   switchport backup mac-address-table update exclude-vlan 10-20,25-30

   When a hyphen (`-`) is used in the VLAN list specification, the value before and the value after the hyphen are counted as two values.

2. Setting the `switchport backup mac-address-table update transmit` command enables this command.

3. Set this command for the primary port.

Related commands

switchport backup interface

switchport backup mac-address-table update transmit

switchport backup mac-address-table update retransmit

Specifies the number of re-transmissions of MAC address update frames.

Syntax

To set or change information:

switchport backup mac-address-table update retransmit *<Count>*

To delete information:

no switchport backup mac-address-table update retransmit

Input mode

`(config-if)`

Parameters

<Count>

Sets the number of re-transmissions of MAC address update frames when the primary port and the secondary port are switched.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3 (times)

Default behavior

MAC address update frames are not re-transmitted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the setting is changed while MAC address update frames are being transmitted, the new value is applied from the next time values are transmitted.
2. Setting the `switchport backup mac-address-table update transmit` command enables this command.
3. Set this command for the primary port.

Related commands

switchport backup interface

switchport backup mac-address-table update transmit

switchport backup mac-address-table update transmit

Enables the sending of MAC address update frames to request that the upstream switches update their MAC address tables.

Syntax

To set information:

switchport backup mac-address-table update transmit

To delete information:

no switchport backup mac-address-table update transmit

Input mode

```
(config-if)
```

Parameters

None

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.

Notes

1. Set this command for the primary port.

Related commands

switchport backup interface

switchport-backup startup-active-port-selection

Enables the functionality to fix the active port at Switch 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 Switch startup.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   primary-only

Default behavior

The secondary port can also be selected as the active port at Switch 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 Switch starts.

Notes

1. Even when this configuration has been deleted, the uplink port on which the functionality to fix the active port at Switch startup is operating 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 functionality to fix the active port at Switch startup is operating, the functionality to fix the active port is released if the following conditions exist:
   - Link-up occurs on the primary port.
   - Execution of the `set switchport-backup active` operation command makes the secondary port the active port.

Related commands

None

32. SML (Split Multi Link) [OS-L2A]

system sml id [OS-L2A]

Sets the device ID to be used for the SML functionality.

Syntax

To set or change information:

system sml id *<sml id>*

To delete information:

no system sml id

Input mode

`(config)`

Parameters

<sml id>

Specify the device ID of SML.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 2

Default behavior

The SML functionality is disabled.

Impact on communication

None

When the change is applied

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

Notes

1. Specify device IDs that are different between two SML devices.
2. When this command is entered, the message below is displayed. These commands become effective after saving all the command settings and then restarting the Switch before entering another configuration command.

   ```
   Please execute the reload after saving all the following commands, because these command become effective after reboot.
    - system sml id
    - system sml peer-link
    - system sml domain
   ```

   You can check the settings of SML by using the `show sml` operation command.

3. The SML functionality cannot be used with Spanning Tree Protocol, Ring Protocol, DHCP snooping, or uplink redundancy functionality. For details about other operations when the SML functionality is enabled, see *18. SML (Split Multi Link) [OS-L2A]* in the *Configuration Guide Vol. 2*.

Related commands

system sml peer-link

system sml domain

system sml domain [OS-L2A]

Sets the SML domain ID.

Syntax

To set or change information:

system sml domain *<domain id>*

To delete information:

no system sml domain

Input mode

`(config)`

Parameters

<domain id>

Specify the SML domain ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 256

Default behavior

The SML functionality is disabled.

Impact on communication

None

When the change is applied

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

Notes

1. Set the two SML devices comprising SML to the same SML domain ID.
2. When this command is entered, the message below is displayed. These commands become effective after saving all the command settings and then restarting the Switch before entering another configuration command.

   ```
   Please execute the reload after saving all the following commands, because these command become effective after reboot.
    - system sml id
    - system sml peer-link
    - system sml domain
   ```

   You can check the settings of SML by using the `show sml` operation command.
3. The SML functionality cannot be used with Spanning Tree Protocol, Ring Protocol, DHCP snooping, or uplink redundancy functionality. For details about other operations when the SML functionality is enabled, see *18. SML (Split Multi Link) [OS-L2A]* in the *Configuration Guide Vol. 2*.

Related commands

system sml id

system sml peer-link

system sml peer-link [OS-L2A]

Sets the peer link port that connects between SML devices.

Syntax

To set or change information:

system sml peer-link interface *<interface id list>*

To delete information:

no system sml peer-link

Input mode

`(config)`

Parameters

interface *<interface id list>*

Specify the port for SML connection.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The following table lists the specifiable values.

	gigabitethernet	**tengigabitethernet**
AX2530S-24T/AX2530S-24TD	0/25 to 0/28	-
AX2530S-24T4X	-	0/25 to 0/28
AX2530S-48T/AX2530S-48TD	0/49 to 0/52	-
AX2530S-48T2X	0/49 to 0/50	0/51 to 0/52
AX2530S-24S4X/AX2530S-24S4XD	-	0/25 to 0/28

You can select up to two peer link ports. Use either of the following combinations. Note that the combination of the first half and the latter half is unavailable.

- First half (For [24T], [24T4X], [24S4X], [24TD], or [24S4XD]: 0/25 to 0/26; For [48T], [48T2X], or [48TD]: 0/49 to 0/50)
- Latter half (For [24T], [24T4X], [24S4X], [24TS], or [24S4XD]: 0/27 to 0/28; For [48T], [48T2X], or [48TD]: 0/51 to 0/52)

Default behavior

The SML functionality is disabled.

Impact on communication

None

When the change is applied

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

Notes

1. In the port set as the peer link with this command, the operation as the peer link takes priority. Therefore, after the Switch is restarted, the other configurations set in the port will be disabled. Also, in the port set as the peer link, the `show running-config` operation command does not display the settings under the interface mode.
2. When this command is entered, the message below is displayed. These commands become effective after saving all the command settings and then restarting the Switch before entering another configuration command.

   ```
   Please execute the reload after saving all the following commands, because these command
   become effective after reboot.

    - system sml id

    - system sml peer-link

    - system sml domain
   ```

   You can check the settings of SML by using the `show sml` operation command.
3. The SML functionality cannot be used with Spanning Tree Protocol, Ring Protocol, DHCP snooping, or uplink redundancy functionality. For details about other operations when the SML functionality is enabled, see *18. SML (Split Multi Link) [OS-L2A]* in the *Configuration Guide Vol. 2*.

Related commands

system sml domain

system sml id

Part 12: High Reliability Based on Network Failure Detection

33. IEEE 802.3ah/UDLD

efmoam active
efmoam disable
efmoam udld-detection-count

efmoam active

Sets the port to be monitored by the IEEE 802.3ah/OAM functionality to active mode.

Syntax

To set or change information:

efmoam active [udld]

To delete information:

no efmoam active

Input mode

`(config-if)`

Parameters

udld

Sets the applicable port as the port to be monitored by the IEEE 802.3ah/UDLD functionality and enables the unidirectional link failure detection functionality.

1. Default value when this parameter is omitted:

   The unidirectional link failure detection functionality is not executed on the applicable port.

2. Range of values:

   None

Default behavior

The applicable port operates in passive mode and does not detect a unidirectional link failure.

Impact on communication

If this functionality is enabled and a line failure is detected, the applicable port is deactivated.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `udld` parameter is not set on both connected ports, link failures cannot be detected by using this functionality.

Related commands

None

efmoam disable

Enables or disables the IEEE 802.3ah/OAM functionality on a switch.

To disable the IEEE 802.3ah/OAM functionality, set the `efmoam disable` command.

To enable the IEEE 802.3ah/OAM functionality again, set the `no efmoam disable` command.

In passive mode, the send process starts when an OAMPDU from the active mode is received.

Syntax

To set information:

```
efmoam disable
```

To delete information:

```
no efmoam disable
```

Input mode

`(config)`

Parameters

None

Default behavior

The IEEE 802.3ah/OAM functionality operates.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

efmoam udld-detection-count

Sets the number of OAMPDU response timeouts that must occur to recognize a failure. (The OAMPDU is a monitoring packet of the IEEE 802.3ah/UDLD functionality.)

Syntax

To set or change information:

efmoam udld-detection-count *<Count>*

To delete information:

no efmoam udld-detection-count

Input mode

`(config)`

Parameters

<Count>

Sets 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 (times)

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

34. Storm Control

storm-control

Configures the storm control functionality. This functionality sets the threshold of frames to be flooded and received by a Switch. When a broadcast storm or another problem occurs, the flooded frames exceeding the threshold are discarded. As a result, network load and Switch load decrease.

The following are specifiable when storm control is used:

- A storm detection threshold (upper threshold), recovery-from-storm threshold, and flow rate limit value (lower threshold) specified as a number of received frames
- Blocking the target port or limiting the flow rate of received frames
- Monitoring time for canceling the flow rate limit
- Issuing SNMP traps or outputting an operation log data

Syntax

To set or change information:

storm-control broadcast level pps *<Packet/s 1>* [*<Packet/s 2>*]

storm-control multicast level pps *<Packet/s 1>* [*<Packet/s 2>*]

storm-control unicast level pps *<Packet/s 1>* [*<Packet/s 2>*]

storm-control action { inactivate | filter }

storm-control action trap

storm-control action log

storm-control filter-broadcast *<Packet/s>*

storm-control filter-multicast *<Packet/s>*

storm-control filter-unicast *<Packet/s>*

storm-control filter-recovery-time *<Seconds>*

To delete information:

no storm-control broadcast

no storm-control multicast

no storm-control unicast

no storm-control action { inactivate | filter }

no storm-control action trap

no storm-control action log

no storm-control filter-broadcast

no storm-control filter-multicast

no storm-control filter-unicast

no storm-control filter-recovery-time

Input mode

`(config-if)`

Parameters

broadcast

Sets broadcast frames as subject to storm control.

1. Default value when this parameter is omitted:

   The storm control functionality is not set.

multicast

Sets multicast frames as subject to storm control.

1. Default value when this parameter is omitted:

   The storm control functionality is not set.

unicast

Sets unicast frames as subject to storm control.

1. Default value when this parameter is omitted:

   The storm control functionality is not set.

level pps *<Packet/s 1>* [*<Packet/s 2>*]

<Packet/s 1>: Sets the storm detection threshold (upper limit) for the number of received frames subject to storm control. Frames exceeding the threshold are discarded. If 0 is set, all applicable frames are discarded.

<Packet/s 2>: Sets a value (recovery-from-storm threshold) used for determining that the Switch has recovered following a storm. If this value is omitted, the storm detection threshold is used as the recovery-from-storm threshold.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See the table below.

Table 34-1 Range of threshold values and the increment step value

Setting range: (pps)	increment step value: (pps)
0 to 1500000	10
1500000 to 10000000	100

action { inactivate | filter }

Sets the Switch operation to be performed when a storm is detected.

inactivate

Deactivates the applicable port. If the port belongs to a channel group, deactivates all ports belonging to the channel group. When this parameter has been set and a port is deactivated 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 traps are issued.

filter

Limits the flow rate of frames received from the applicable port. If the port belongs to a channel group, only the port itself is subject to the limit.

1. Default value when this parameter is omitted:

   If a storm is detected, only the frames exceeding the storm detection threshold are deleted. The port status does not change.

2. Range of values:

   `inactivate` or `filter`

action trap

Issues an SNMP trap when a storm or the end of a storm is detected.

1. Default value when this parameter is omitted:

   If a storm is detected, no SNMP traps are issued.

action log

Outputs operation log data when a storm or the end of a storm is detected.

1. Default value when this parameter is omitted:

   Operation log data is not output when a storm is detected.

filter-broadcast *<Packet/s>*

When the flow rate of broadcast frames has a limit, this parameter sets the limit value (lower threshold) as the number of broadcast frames that can be forwarded. The frames exceeding the flow rate limit value are discarded. If 0 is set, all applicable frames are discarded.

1. Default value when this parameter is omitted:

   When the flow rate has a limit, all broadcast frames are discarded.

2. Range of values:

Table 34-2 Range of threshold values and the increment step value

Setting range: (pps)	**increment step value: (pps)**
0 to 1500000	10
1500000 to 10000000	100

filter-multicast *<Packet/s>*

When the flow rate of multicast frames has a limit, this parameter sets the limit value (lower threshold) as the number of multicast frames that can be forwarded. The frames exceeding the flow rate limit value are discarded. If 0 is set, all applicable frames are discarded.

1. Default value when this parameter is omitted:

   When the flow rate has a limit, all multicast frames are discarded.

2. Range of values:

Table 34-3 Range of threshold values and the increment step value

Setting range: (pps)	**increment step value: (pps)**
0 to 1500000	10
1500000 to 10000000	100

filter-unicast *<Packet/s>*

When the flow rate of unknown unicast frames has a limit, this parameter sets the limit value (lower threshold) as the number of unknown unicast frames that can be forwarded. The frames that drop below the flow rate limit value (lower threshold) are discarded. If 0 is set, all applicable frames are discarded.

1. Default value when this parameter is omitted:

   When the flow rate has a limit, all unknown unicast frames are discarded.

2. Range of values:

Table 34-4 Range of threshold values and the increment step value

Setting range: (pps)	increment step value: (pps)
0 to 1500000	10
1500000 to 10000000	100

filter-recovery-time *<Seconds>*

Sets the monitoring time for cancellation of the flow rate limit after flow rate limit has gone into effect due to the detection of a storm. The monitoring time begins when the number of received frames drops below the recovery-from-storm threshold, and the flow rate limit is canceled when the time expires.

1. Default value when this parameter is omitted:

   The initial value is 1 second.

2. Range of values:

   1 to 30 (seconds)

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 received frames exceed the storm detection threshold, control frames are also discarded. To prevent necessary control frames from being discarded, do not specify too small a value.
3. When the number of received frames exceeds the storm detection value set by using `storm-control broadcast`, `storm-control multicast`, or `storm-control unicast`, the operation set for `storm-control action` is treated as detection of a storm. If the number of received frames drops below the storm detection threshold after a storm is detected, the Switch is considered to have recovered from the storm. If a storm detection threshold has not been set, the operation set for `storm-control action` is not performed.
4. When `storm-control action inactivate` is set, if a storm has been detected and the port is deactivated, use the `activate` operation command to activate the port. If a storm is detected and a port is deactivated, no frames are received. In this state, the end of the storm cannot be detected.
5. When using SNMP traps, you must use the `snmp-server host` command to set the destination IP address and `storm-control`.

Related commands

snmp-server host

35. L2 Loop Detection

loop-detection

Sets the port type for the L2 loop detection functionality.

Syntax

To set or change information:

loop-detection { send-inact-port | send-port | uplink-port | exception-port }

To delete information:

no loop-detection

Input mode

```
(config-if)
```

Parameters

{ send-inact-port | send-port | uplink-port | exception-port }

send-inact-port

Sets a port as a detecting and blocking port. When an L2 loop detection frame is sent and an L2 loop detection frame sent from the local Switch is received, log data is output and the port is blocked.

send-port

Sets a port as a detecting and sending port. When an L2 loop detection frame is sent and an L2 loop detection frame sent from the local switch is received, log data is output.

uplink-port

Sets a port as an uplink port. No L2 loop detection frames are sent. When an L2 loop detection frame from the local switch is received, log data is output to the frame source. If the port type of the frame source is detecting and blocking port, the frame source is blocked.

exception-port

Sets a port as exempt from L2 loop detection. When an L2 loop detection frame is received, no operation is performed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   send-inact-port, send-port, uplink-port, exception-port

Default behavior

The port operates as a detecting port. If an L2 loop detection frame is not sent and an L2 loop detection frame sent from the local switch is detected, log data is output.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Changing the port type clears the following information:

- The number of L2 loop detections until the port is blocked
- The time from blocking of the port until automatic recovery occurs.

2. 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 until a blocked 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 blocked port is activated automatically.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   60 to 86400 (seconds)

Default behavior

A blocked 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 operational only after the remaining time has been cleared.

Related commands

loop-detection enable

loop-detection enable

Enables L2 loop detection.

Syntax

To set information:

```
loop-detection enable
```

To delete information:

```
no loop-detection enable
```

Input mode

`(config)`

Parameters

None

Default behavior

L2 loop detection 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

Sets the time for holding the number of L2 loop detections before a port is blocked.

If the period of time for holding the number of L2 loop detections elapses without an L2 loop detection frame being received since the last L2 loop detection frame was received, the number of L2 loop detections held on the port is cleared.

Syntax

To set or change information:

loop-detection hold-time *<Seconds>*

To delete information:

no loop-detection hold-time

Input mode

```
(config)
```

Parameters

<Seconds>

Sets the period of time in seconds for holing the number of L2 loop detections.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 86400 (seconds)

Default behavior

The number of L2 loop detections continue to be held.

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 any time remains for holding the number of L2 loop detections, the change becomes operational only after the remaining time has been cleared.

Related commands

loop-detection enable

loop-detection interval-time

Sets the interval for sending L2 loop detection frames.

Syntax

To set or change information:

loop-detection interval-time *<Seconds>*

To delete information:

no loop-detection interval-time

Input mode

`(config)`

Parameters

<Seconds>

Sets the interval (in seconds) for sending L2 loop detection frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600 (seconds)

Default behavior

The interval for sending L2 loop detection frames is 10 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

loop-detection enable

loop-detection threshold

Sets the number of L2 loop detections before a port is blocked. If the number of detections becomes equal to or greater than the specified number, the port is blocked.

Syntax

To set or change information:

loop-detection threshold *<Count>*

To delete information:

no loop-detection threshold

Input mode

`(config)`

Parameters

<Count>

Sets the number of L2 loop detections before a port is blocked.

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 detections before a port is blocked is 1.

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 any L2 loop detections still remain, the change becomes operational only after the remaining number of detections has been cleared.

Related commands

loop-detection enable

36. CFM

domain name

Sets the name used for the applicable 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>*

Use a character string that is no more than 43 characters to set 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:

   Specify a character string that is no more than 43 characters for *<Strings>*. For details about the characters that can be specified, see *Specifiable values for parameters*.

   Specify a character string that is no more than 63 characters for *<Name>*. The firtst character must be an alphabetical character. Subsequent characters can be alphanumeric characters, hyphens (`-`), and periods (`.`).

   Specify a value from `0000.0000.0000` to `feff.ffff.ffff` for *<Mac>*. Note, however, that a multicast MAC address (address whose first-byte lower bit is set to 1) cannot be set.

   Specify a value from `0` to `65535` for *<ID>*.

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

None

Related commands

ethernet cfm domain

ethernet cfm cc alarm-priority

Sets the failure level to be detected by CC.

Failure levels equal to or higher than the parameter you set are 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.>*

Sets the MA ID number set by using the `ma` 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

alarm-priority *<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 shows levels detected by CC and failure descriptions.

Table 36-1 Levels detected by CC and failures descriptions

Setting level	Failure type	Command display	Failure description
5	DefXconCCM	OtherCCM	A CCM with a different domain and MA was received.

Setting level	Failure type	Command display	Failure description
4	DefErrorCCM	ErrorCCM	A CCM with an incorrect MEP ID or transmission interval was received.
3	DefRemoteCCM	Timeout	CCMs are no longer being received.
2	DefMACstatus	PortState	The port on the target Switch cannot communicate.
1	DefRDICCM	RDI	A CCM that reported the detection of a failure was received. Remote Defect Indication
0	none	-	No failure was detected.

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 domain

ma name

ma vlan-group

ethernet cfm cc alarm-reset-time

Sets the time interval for identifying re-detection when CC repeatedly detects failures. If a failure is detected within the time set by using this command after a failure has been detected, the failure is treated as a re-detection and no trap is sent.

Note, however, that if a failure with a failure level higher than the currently detected failure level is detected, a trap is sent.

Syntax

To set or change information:

ethernet cfm cc level *<Level>* ma *<No.>* alarm-reset-time *<Time>*

To delete information:

no ethernet cfm cc level *<Level>* ma *<No.>* alarm-reset-time

Input mode

`(config)`

Parameters

level *<Level>*

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma *<No.>*

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

alarm-reset-time *<Time>*

Sets the time for re-detecting a failure.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Multiples of 100 from 2500 to 10000 in milliseconds

Default behavior

The maximum time for treatment as a re-detection is 10000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If higher level MAs are not included as lower level MAs, a communication overload might occur.

Related commands

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc alarm-start-time

Sets the time after CC detects a failure until a trap is sent.

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

alarm-start-time *<Time>*

Sets the time until a trap is sent following detection of a failure.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Multiples of 100 from 2500 to 10000 in milliseconds

Default behavior

2500 milliseconds are used as the time until a trap is sent following detection of a failure.

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 enable

Sets in a domain an MA in which the CC functionality is used.

If the `ethernet cfm mep` command has already been set, sending from the applicable port to CCM starts.

Syntax

To set information:

ethernet cfm cc level *<Level>* ma *<No.>* enable

To delete information:

no ethernet cfm cc level *<Level>* ma *<No.>* enable

Input mode

`(config)`

Parameters

level *<Level>*

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma *<No.>*

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

Monitoring by CC is not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ethernet cfm domain

ma name

ma vlan-group

ethernet cfm cc interval

Sets the CCM transmission interval for a target MA.

Syntax

To set or change information:

ethernet cfm cc level *<Level>* ma *<No.>* interval {1s | 10s | 1min | 10min}

To delete information:

no ethernet cfm cc level *<Level>* ma *<No.>* interval

Input mode

`(config)`

Parameters

level *<Level>*

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma *<No.>*

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command. Even if the `ma name` command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

interval {1s | 10s | 1min | 10min}

Sets the interval for sending CCMs.

1s

Sets the interval for sending CCMs to 1 second.

10s

Sets the interval for sending CCMs to 10 seconds.

1min

Sets the interval for sending CCMs to 1 minute.

10min

Sets the interval for sending CCMs to 10 minutes.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `1s`, `10s`, `1min`, or `10min`

3. Note on using this parameter:

   If a value smaller than the default value is set for this parameter, the Switch CPU becomes overloaded with possible adverse effects on communication.

Default behavior

`1min` is used as the interval for sending CCMs.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

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>*

Sets the domain level.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

direction-up

When up/down is not explicitly set by using the `ethernet cfm mep` command, you can set this parameter to have the Switch operate in Up MEP mode.

1. Default value when this parameter is omitted:

   The Switch operates in Down MEP mode.

2. Range of values:

   None

3. Note on using this parameter:

   This parameter cannot be changed. If you want to change the parameter, delete the applicable command first, and then set the parameter.

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

None

ethernet cfm enable (global)

Starts CFM.

Syntax

To set information:

```
ethernet cfm enable
```

To delete information:

```
no ethernet cfm enable
```

Input mode

`(config)`

Parameters

None

Default behavior

CFM does not operate even if another CFM command has been set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

ethernet cfm enable (interface)

When `no ethernet cfm enable` is set, CFM PDU transmission processing on the applicable port or the applicable port channel stops.

Syntax

To set information:

```
no ethernet cfm enable
```

To delete information:

```
ethernet cfm enable
```

Input mode

`(config-if)`

Parameters

None

Default behavior

CFM PDUs can be received.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

None

ethernet cfm mep

Sets a MEP used by the CFM functionality.

Syntax

To set information:

ethernet cfm mep level *<Level>* ma *<No.>* mep-id *<MEPID>* [{down | up}]

To delete information:

no ethernet cfm mep level *<Level>* ma *<No.>* mep-id *<MEPID>*

Input mode

`(config-if)`

Parameters

level *<Level>*

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma *<No.>*

Specifies an MA ID number that has been set by using the `ma name` command or the `ma vlan-group` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

mep-id *<MEPID>*

Sets the MEP ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8191

3. Note on using this parameter:

   Set a value unique within the MA.

{down | up}

Specifies the direction of a domain.

down

Sets the MEP as Down MEP so that the line side will be maintained.

up

Sets the MEP as Up MEP so that the relay side (toward the switch) will be maintained.

1. Default value when this parameter is omitted:

When `direction-up` has been set by using the `ethernet cfm domain` command, Up MEP is used. If it has not been set, Down MEP is used.

2. Range of values:

   `down` or `up`

3. Note on using this parameter:

   This parameter cannot be changed. If you want to change this parameter, delete this configuration first, and then reset it.

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 domain

ethernet cfm mip

Sets a MIP used by the CFM functionality.

Syntax

To set information:

ethernet cfm mip level *<Level>*

To delete information:

no ethernet cfm mip level *<Level>*

Input mode

`(config-if)`

Parameters

level *<Level>*

Specifies the domain level that has been set by using the `ethernet cfm domain` command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the `ethernet cfm mep` command is set on the same interface, a domain level equal to or lower than the `ethernet cfm mep` command cannot be specified.
2. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

Related commands

ethernet cfm domain

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.>

Sets 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:

   Specify a character string that is no more than 45 characters for *<Strings>*. For details about the characters that can be specified, see *Specifiable values for parameters*.

   Specify a value from 1 to 4094 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 that is 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 set.

Default behavior

<No.> of the `ma vlan-group` command is used for a name of an MA.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ethernet cfm domain

ma vlan-group

Sets the VLAN belonging to the MA used in the applicable 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.>

Sets 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>

Sets the VLANs to be used in the applicable MA.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set *<VLAN ID List>* and the specifiable values, see *Specifiable values for parameters*.

primary-vlan *<VLAN ID>*

Sets 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:

   The VLAN IDs specified by using `vlan-group` *<VLAN ID List>* are set.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

ethernet cfm domain

Part 13: Remote Network Management

37. 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 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:

   Specify a character string that is no more than 60 characters. For details about the characters that can be specified, see *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

rmon alarm

Sets the control information for the RMON (RFC 1757) alarm group. This command can configure a maximum of 128 entries.

Syntax

To set or change information:

rmon alarm *<Number>* *<Variable>* *<Interval>* {delta | absolute} rising-threshold *<Value>* rising-event-index *<Event#>* falling-threshold *<Value>* falling-event-index *<Event#>* [owner *<Owner string>*] [startup_alarm { rising_falling | rising | falling }]

To delete information:

no rmon alarm *<Number>*

Input mode

`(config)`

Parameters

<Number>

Sets 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>

Sets 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 as follows:

   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.

   - Object name

     See *Table 37-1 The setting range of object identifiers subject to alarm monitoring*.

   - Instance number

     `x` in *Table 37-1 The setting range of object identifiers subject to alarm monitoring* is the instance number, which sets `ifIndex` of the MIB. For details about the range of `ifIndex`, see the manual *MIB Reference*.

Table 37-1 The setting range of object identifiers subject to alarm monitoring

Object name (setting range from the console)	**Object ID (setting value from the SNMP manager)**
ifInOctets.*x*	1.3.6.1.2.1.2.2.1.10.*x*
ifInUcastPkts.*x*	1.3.6.1.2.1.2.2.1.11.*x*
ifInNUcastPkts.*x*	1.3.6.1.2.1.2.2.1.12.*x*
ifInDiscards.*x*	1.3.6.1.2.1.2.2.1.13.*x*
ifInErrors.*x*	1.3.6.1.2.1.2.2.1.14.*x*
ifInUnknownProtos.*x*	1.3.6.1.2.1.2.2.1.15.*x*
ifOutOctets.*x*	1.3.6.1.2.1.2.2.1.16.*x*
ifOutUcastPkts.*x*	1.3.6.1.2.1.2.2.1.17.*x*
ifOutNUcastPkts.*x*	1.3.6.1.2.1.2.2.1.18.*x*
ifOutDiscards.*x*	1.3.6.1.2.1.2.2.1.19.*x*
ifOutErrors.*x*	1.3.6.1.2.1.2.2.1.20.*x*
etherStatsDropEvents.*x*	1.3.6.1.2.1.16.1.1.1.3.*x*
etherStatsOctets.*x*	1.3.6.1.2.1.16.1.1.1.4.*x*
etherStatsPkts.*x*	1.3.6.1.2.1.16.1.1.1.5.*x*
etherStatsBroadcastPkts.*x*	1.3.6.1.2.1.16.1.1.1.6.*x*
etherStatsMulticastPkts.*x*	1.3.6.1.2.1.16.1.1.1.7.*x*
etherStatsCRCAlignErrors.*x*	1.3.6.1.2.1.16.1.1.1.8.*x*
etherStatsUndersizePkts.*x*	1.3.6.1.2.1.16.1.1.1.9.*x*
etherStatsOversizePkts.*x*	1.3.6.1.2.1.16.1.1.1.10.*x*
etherStatsFragments.*x*	1.3.6.1.2.1.16.1.1.1.11.*x*
etherStatsJabbers.*x*	1.3.6.1.2.1.16.1.1.1.12.*x*
etherStatsCollisions.*x*	1.3.6.1.2.1.16.1.1.1.13.*x*
etherStatsPkts64Octets.*x*	1.3.6.1.2.1.16.1.1.1.14.*x*
etherStatsPkts65to127Octets.*x*	1.3.6.1.2.1.16.1.1.1.15.*x*
etherStatsPkts128to255Octets.*x*	1.3.6.1.2.1.16.1.1.1.16.*x*
etherStatsPkts256to511Octets.*x*	1.3.6.1.2.1.16.1.1.1.17.*x*
etherStatsPkts512to1023Octets.*x*	1.3.6.1.2.1.16.1.1.1.18.*x*

Object name (setting range from the console)	**Object ID (setting value from the SNMP manager)**
etherStatsPkts1024to1518Octets.*x*	1.3.6.1.2.1.16.1.1.1.19.*x*
ifInMulticastPkts.*x*	1.3.6.1.2.1.31.1.1.1.2.*x*
ifInBroadcastPkts.*x*	1.3.6.1.2.1.31.1.1.1.3.*x*
ifOutMulticastPkts.*x*	1.3.6.1.2.1.31.1.1.1.4.*x*
ifOutBroadcastPkts.*x*	1.3.6.1.2.1.31.1.1.1.5.*x*

x: instance number

<Interval>

Sets 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 (seconds)

{ delta | absolute }

Sets the method for checking the threshold. If `delta` is specified, the difference between the current value and the value of the last sampling is compared with the threshold. If `absolute` is specified, the current value is compared directly with the threshold. This parameter is equivalent to `alarmSampleType` defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `delta` or `absolute`

rising-threshold *<Value>*

Sets 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#>*

Sets 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 set by using the `rmon event` 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 in the control information set by using the `rmon event` command for *<Event#>*.

falling-threshold *<Value>*

Sets 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#>*

Sets the identification number of the method for generating an event if a value drops below the lower threshold. The method for generating an event is the information identification number set by using the `rmon event` 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 in the control information set by using the `rmon event` command for *<Event#>*.

owner *<Owner string>*

Sets 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:

   Specify a character string that is no more than 24 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

startup_alarm { rising_falling | rising | falling }

Sets the timing for checking the threshold in the first sampling. If `rising` is set, an alarm is generated when the upper threshold is exceeded in the first sampling. If `falling` is set, an alarm is generated when a value drops below the lower threshold in the first sampling. If `rising_falling` is specified, an alarm is generated when the upper or lower threshold is crossed in the first sampling. This parameter is equivalent to `alarmstartUpAlarm` defined in RFC 1757.

1. Default value when this parameter is omitted:

   rising_falling

2. Range of values:

   rising, falling, or rising_falling

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To access an alarm group from the SNMP manager, you must register the SNMP manager by using the `snmp-server community` command.
2. As the value for `rising-event-index` or `falling-event-index` of an alarm group, set the information identification number that has been set for the corresponding event group.
3. When setting this command from a console, you must use an object name. If you use an object ID for setting this command from the SNMP manager, and you execute the `show running-config` operation command on the console, the object name is displayed.

Related commands

snmp-server host

rmon event

rmon collection history

Configures the control information for the RMON (RFC 1757) Ethernet statistics history. This command can configure a maximum of 32 entries.

Syntax

To set or change information:

rmon collection history controlEntry *<Integer>* [owner *<Owner name>*] [buckets *<Bucket number>*] [interval *<Seconds>*]

To delete information:

no rmon collection history controlEntry *<Integer>*

Input mode

`(config-if)`

Parameters

<Integer>

Sets 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>*

Sets 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:

   Specify a character string that is no more than 24 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

buckets *<Bucket number>*

Sets 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 set for *<Bucket number>*, operation is the same as if 50 had been set.

interval *<Seconds>*

Sets the time interval (in seconds) for collecting statistics. This parameter is equivalent to `historyControlInterval` defined in RFC 1757.

1. Default value when this parameter is omitted:

1800 (seconds)

2. Range of values:

   1 to 3600 (seconds)

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. If an entry is added or deleted by using this command, the Ethernet History group information obtained by an SNMP manager might temporarily become indefinite values.

Related commands

interface

snmp-server community

rmon event

Sets the control information for an RMON (RFC 1757) event group. This command can configure a maximum of 16 entries.

Syntax

To set or change information:

rmon event *<Event#>* [log] [trap *<Community>*] [description *<Description string>*] [owner *<Owner string>*]

To delete information:

no rmon event *<Event#>*

Input mode

`(config)`

Parameters

<Event#>

Sets 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 sets the method for generating alarms and sends SNMP traps to the community specified for *<Community>* or SNMPv3 users. This parameter is equivalent to `eventCommunity` defined in RFC 1757.

1. Default value when this parameter is omitted:

   No traps are sent.

2. Range of values:

   Sets `trap` and the community name.

   Specify a character string that is no more than 60 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

description *<Description string>*

Uses a character string to set 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:

   Specify a character string that is no more than 79 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

owner *<Owner string>*

Sets 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:

   Specify a character string that is no more than 24 characters. For details about the characters that can be specified, 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. When an event group is accessed from the SNMP manager and traps 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 a trap to the SNMP manager, set the IP address of the SNMP manager and `rmon` by using the `snmp-server host` command.
3. A trap 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.

Related commands

snmp-server host

rmon alarm

snmp-server community

Sets the access list for the SNMP community. The command can configure up to 50 entries.

Syntax

To set or change information:

snmp-server community *<string>* [{ro|rw}] [*<access list name>*]

To delete information:

no snmp-server community *<string>*

Input mode

`(config)`

Parameters

<string>

Sets the community name for the SNMP manager.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

{ro | rw}

Sets the MIB operating mode for the manager whose IP address belongs to the community that has been set. If `ro` is set, `Get Request`, `GetNext Request`, and `GetBulkRequest` are permitted. If `rw` is set, `Get Request`, `GetNext Request`, `GetBulkRequest`, and `Set Request` are permitted.

1. Default value when this parameter is omitted:

   ro

2. Range of values:

   ro or rw

<access list name>

Sets the name of IPv4 address filter or IPv6 address filter in which the permissions for this community are set. If *<access list name>* is omitted, all accesses are permitted. In addition, if *<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:

   None.(All accesses are permitted.)

2. Range of values:

   Specify an access list name that is 4 to 31 characters. For details about the characters that can be specified, 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 an IPv4 address filter is set, access in IPv6 environments is not permitted.
2. If an IPv6 filter is set, access in IPv4 environments is not permitted.

Related commands

ip access-list standard

ipv6 access-list

snmp-server contact

Sets the contact information of the Switch.

Syntax

To set or change information:

snmp-server contact *<Text>*

To delete information:

no snmp-server contact

Input mode

`(config)`

Parameters

<Text>

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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string that is no more than 60 characters. For details about the characters that can be specified, see *Specifiable values for parameters*.

Default behavior

The initial value is null.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about `name`, `contact`, and `location` from the SNMP manager, you must use the `snmp-server community` command to register the SNMP manager.

Related commands

None

snmp-server engineID local

Sets SNMP engine ID information.

Syntax

To set or change information:

snmp-server engineID local *<engineid string>*

To delete information:

no snmp-server engineID local

Input mode

`(config)`

Parameters

<engineid string>

Sets an SNMP engine ID.

The SNMP engine ID value set for a Switch is as follows:

1st to 4th octets: 0x8000554F

5th octet: 0x04

6th to 32nd and after octets: Setting value for *<engineid string>*

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 27 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The SNMP engine ID value set for a Switch is as follows:

1st to 4th octets: 0x8000554F

5th octet: 0x80

6th to 9th octets: A pseudo-random number

10th to 13th octets: Time when the ID is automatically generated (Total number of seconds from 1970)

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can check the SNMP engine ID settings with the `show snmp engineID local` operation command.

2. When the SNMP engine ID is changed, if the Switch is restarted without the configuration saved, the number of restart times only is reset and the SNMPv3 authentication might not properly work. In that case, set again and save the SNMP engine ID, and then restart the Switch.
3. If the Switch unexpectedly restarts, the SNMP engine ID or the number of restart times after the SNMP engine ID is changed might be corrupted in bits. In that case, recovery is possible with the `set snmp-server engineID local` operation command.
4. If multiple users have been registered, it takes several tens of seconds to change the SNMP engine ID.

Related commands

snmp-server view

snmp-server user

snmp-server group

snmp-server host

snmp-server group

Sets SNMP security group information. A maximum of 50 group names can be set by this command.

Syntax

To set or change information:

snmp-server group *<group name>* v3 { noauth | auth | priv } [read *<view name>*] [write *<view name>*] [notify *<view name>*]

To delete information:

no snmp-server group *<group name>* v3 { noauth | auth | priv }

Input mode

`(config)`

Parameters

<group name>

Configures an SNMP security group name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

{ noauth | auth | priv }

This is the security level to be requested in order to give permission to access MIB view specified by the Read view, Write view or Notify view parameter.

If the security level of a send and receive message is lower than that set with this parameter, access permission is not given.

If multiple security levels are set using the same SNMP security group name, access is controlled in the MIB view with the highest security level among the security levels equal to or lower than that of a send and receive message.

`noauth`: Authentication and encryption are not required.

`auth`: Authentication is required, and encryption is not required.

`priv`: Authentication and encryption are both required.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   `noauth`, `auth`, or `priv`

read *<view name>*

Sets the MIB view name to be used for access control when receiving SNMP packets of any of the following PDU types.

- GetRequest-PDU

- GetNextRequest-PDU
- GetBulkRequest-PDU

1. Default value when this parameter is omitted:

   The read access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

write *<view name>*

Sets the MIB view name to be used for access control when receiving SNMP packets of `SetRequest-PDU` type.

1. Default value when this parameter is omitted:

   The write access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

notify *<view name>*

Sets the MIB view name to be used for access control when sending a trap.

A trap is not sent unless the object identifier of the trap itself and the object identifiers included in the trap are all accessible.

1. Default value when this parameter is omitted:

   The notify access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a MIB view name that has not been set by the `snmp-server view` command is set for the read view name, write view name, or notify view name of this command, the

view name information set by this command is empty.

2. To generate a trap, the notify view name information of this command and the `snmp-server host` command setting are required.

Related commands

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server host

snmp-server host

Registers the network management switch (SNMP manager) to which traps are sent. This command can configure a maximum of 50 entries.

Syntax

To set or change information:

snmp-server host *<manager address>* traps *<string>* [version { 1 | 2c | 3 { noauth | auth | priv } }] [snmp] [rmon] [air-fan] [power] [login] [temperature] [axrp] [storm-control] [efmoam] [dot1x] [web-authentication] [mac-authentication] [loop-detection] [switchport-backup] [cfm] [sml]

To delete information:

no snmp-server host *<manager address>*

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).

   IPv4 unicast address

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   IPv6 global unicast addresses

   ::2 to fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff, fec0:: to feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<string>

For SNMPv1 and SNMPv2C, this parameter sets the name of the community for the SNMP manager.

For SNMPv3, this parameter sets the security user name.

Do not use the at mark (`@`) for the security user name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set a character string within 60 characters with double-quotes for SNMPv1 and SNMPv2C, and a character string within 32 characters with double-quotes for SNMPv3. Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

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

Sets the version for sending the traps of the manager whose IP address belongs to the community that has been set. If 1 is specified, the SNMPv1 version traps are issued. If 2c is specified, SNMPv2C version traps are issued. If 3 is specified, SNMPv3 version traps are issued.

If 3 is specified, this parameter also sets the security level for sending the traps.

- If noauth is specified, traps are sent without authentication and encryption required.
- If auth is specified, traps are sent with authentication required and without encryption required.
- If priv is specified, traps are sent with both authentication and encryption required.

1. Default value when this parameter is omitted:

   1

2. Range of values:

   Specify 1, 2c, or 3.

   If you specify 3, then specify noauth, auth, or priv.

[snmp] [rmon] [air-fan] [power] [login] [temperature] [axrp] [storm-control] [efmoam] [dot1x] [web-authentication] [mac-authentication] [loop-detection] [switchport-backup] [cfm] [sml]

By setting each parameter, you can select the traps to be sent. The following table describes traps that will be sent when parameters are set.

Table 37-2 Correspondence between parameters and traps

Parameter	Traps
snmp	coldStart
	warmStart
	linkUp
	linkDown
	authenticationFailure
rmon	risingAlarm
	fallingAlarm
temperature	ax2530sTemperatureTrap
air-fan	ax2530sAirFanStopTrap
power	ax2530sPowerSupplyFailureTrap
login	ax2530sLoginSuccessTrap
	ax2530sLoginFailureTrap
	ax2530sLogoutTrap
axrp	ax2530sAxrpStateTransitionTrap
	ax2530sAxrpMultiFaultDetectionStartTrap

Parameter	Traps
	ax2530sAxrpMultiFaultDetectionStateTransitionTrap
storm-control	ax2530sBroadcastStormDetectTrap
	ax2530sMulticastStormDetectTrap
	ax2530sUnicastStormDetectTrap
	ax2530sBroadcastStormPortInactivateTrap
	ax2530sMulticastStormPortInactivateTrap
	ax2530sUnicastStormPortInactivateTrap
	ax2530sBroadcastStormRecoverTrap
	ax2530sMulticastStormRecoverTrap
	ax2530sUnicastStormRecoverTrap
efmoam	ax2530sEfmoamUdldPortInactivateTrap
dot1x	ax2530sDot1xFailureTrap
	ax2530sDot1xEventTrap
web-authentication	ax2530sWauthFailureTrap
	ax2530sWauthEventTrap
	ax2530sWauthSystemTrap
mac-authentication	ax2530sMauthFailureTrap
	ax2530sMauthEventTrap
	ax2530sMauthSystemTrap
loop-detection	ax2530sL2ldLinkDown
	ax2530sL2ldLinkUp
	ax2530sL2ldLoopDetection
switchport-backup	ax2530sUlrChangeSecondary
	ax2530sUlrChangePrimary
cfm	dot1agCfmFaultAlarm
sml	ax2530sSmlStatusFull [OS-L2A] ax2530sSmlStatusStandalone [OS-L2A] ax2530sSmlStatusConflict [OS-L2A]

Parameter	Traps
	ax2530sSmlPeerlinkNormal [OS-L2A] ax2530sSmlPeerlinkFailure [OS-L2A] ax2530sSmlPeerlinkRecovery [OS-L2A] ax2530sSmlPeerlinkDisconnect [OS-L2A]

snmp

coldStart, warmStart, linkDown, linkUp, and authenticationFailure traps are sent.

rmon

A trap is sent when the value exceeds the upper threshold or drops below the lower threshold of the rmon alarm.

air-fan

A trap is sent when a fan stops.

power

A trap is sent when a failure occurs in a power supply unit.

login

A trap is sent when a login fails or succeeds or when a logout occurs.

temperature

A trap is sent when the temperature changes.

axrp

A trap is sent when the ring failure monitoring status is changed.

storm-control

A trap is sent when a storm is detected by the storm control functionality or when a Switch recovers from a storm.

efmoam

A trap is sent when a unidirectional link failure is detected.

dot1x

A trap is sent for specific types of authentication accounting log data during IEEE 802.1X authentication.

web-authentication

A trap is sent for specific types of authentication accounting log data during Web authentication.

mac-authentication

A trap is sent for specific types of authentication accounting log data during MAC-based authentication.

loop-detection

A trap is sent when an L2 loop is detected.

switchport-backup

A trap is sent if a line is switched due to uplink redundancy.

cfm

A trap is sent when a failure is detected by CC.

sml [OS-L2A]

A trap related to the SML status or peer link information is sent.

1. Default value when this parameter is omitted:

   No traps corresponding to those parameters are issued.

2. Range of values:

   snmp, rmon, air-fan, power, login, temperature, axrp, tstorm-control, efmoam, dot1x, web-authentication, mac-authentication, loop-detection, switchport-backup, cfm, sml

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the list of supported MIBs and supported traps, see the manual *MIB Reference*.
2. For details about the conditions for issuing private traps for specific types of authentication accounting log data and each authentication functionality (IEEE 802.1X, Web authentication, and MAC-based authentication), see the description about the accounting functionality of each type of authentication in the *Configuration Guide Vol. 2*.
3. `air-fan` can be set only for models with a fan.
4. `127.*.*.*` cannot be specified to *<manager address>* as an IPv4 address.

Related commands

snmp-server engineID local

snmp-server view

snmp-server user

snmp-server group

snmp-server location

Sets the name of the location where the Switch is installed.

Syntax

To set or change information:

snmp-server location *<Text>*

To delete information:

no snmp-server location

Input mode

`(config)`

Parameters

<Text>

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.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

Default behavior

The initial value is null.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about `name`, `contact`, and `location` from the SNMP manager, you must use the `snmp-server community` command to register the SNMP manager.

Related commands

None

snmp-server traps

Sets the timing for issuing a trap.

Syntax

To set or change information:

snmp-server traps [{ limited_coldstart_trap | unlimited_coldstart_trap }]
[link_trap_bind_info {private | standard}] [agent-address *<Agent address>*]
[dot1x-trap {failure | all}] [web-authentication-trap {failure | all}]
[mac-authentication-trap {failure | all}]

To delete information:

no snmp-server traps

Input mode

`(config)`

Parameters

{ limited_coldstart_trap | unlimited_coldstart_trap }

Limits the times when `coldStart Trap` is issued. The following table provides an overview of the events that cause the `coldStart Trap` set by using this parameter to be issued.

Table 37-3 Events causing coldStart Trap to be issued for each parameter

Parameter	Events causing coldStart Trap
limited_coldstart_trap	● A Switch is started (the Switch is turned on).
unlimited_coldstart_trap	● A Switch is started (the Switch is turned on). ● An IP configuration is added or deleted. ● When the time is changed by using the `set clock` command

1. Default value when this parameter is omitted:

   limited_coldstart_trap

2. Range of values:

   limited_coldstart_trap or unlimited_coldstart_trap

link_trap_bind_info {private | standard}

Configures the MIB to be added when `link up/down Trap` is issued.

The following table describes the MIBs to be added when `link up/down Trap` set by using this parameter is issued.

Table 37-4 MIBs to be added when link up/down Trap is issued for each parameter

Parameter	MIBs to be added when link up/down Trap is issued
private	● (Common to SNMPv1, SNMPv2C, and SNMPv3 traps) `ifIndex`, `ifDescr`, and `ifType`
standard	● (For SNMPv1 traps) `ifIndex` ● (For SNMPv2C/SNMPv3) `ifIndex`, `ifAdminStatus`, and `ifOperStatus`

1. Default value when this parameter is omitted:

   standard

2. Range of values:

   `private` or `standard`

agent-address *<Agent address>*

Sets the IPv4 address to be used for *<Agent address>* in a trap notification frame in SNMPv1 format. Because only the SNMPv1 frame format can have the *<Agent address>* field in their Trap-PDUs, the address set by using this command is applied to SNMPv1 traps.

1. Default value when this parameter is omitted:

   If this parameter is not set, the VLAN ID's IPv4 address whose *<Agent address>* value is the smallest in the trap notification frame is used.

2. Range of values:

   Set an IPv4 address from `0.0.0.0` to `255.255.255.255` for *<Agent address>*.

dot1x-trap {failure | all}

Sets the trap type for IEEE 802.1X authentication.

failure

Only traps for an authentication failure are issued.

all

Traps for successful authentications, failed authentications, or canceled authentications are issued.

1. Default value when this parameter is omitted:

   failure

2. Range of values:

   `failure` or `all`

web-authentication-trap {failure | all}

Sets the trap type for Web authentication.

failure

Only traps for an authentication failure are issued.

all

Traps for successful authentications, failed authentications, or canceled authentications are issued.

1. Default value when this parameter is omitted:

   failure

2. Range of values:

   `failure` or `all`

mac-authentication-trap {failure | all}

Sets the trap type for MAC-based authentication.

failure

Only traps for an authentication failure are issued.

all

Traps for successful authentications, failed authentications, or canceled authentications are issued.

1. Default value when this parameter is omitted:

failure

2. Range of values:

   `failure` or `all`

Default behavior

The initial values for all parameters of this command are used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the list of supported MIBs and supported traps, see the manual *MIB Reference*.
2. You cannot omit all of the parameters in this command. You must set at least one.

Related commands

None

snmp-server user

Sets SNMP security user information. This command can configure a maximum of 50 entries.

This command configures the authentication protocol and the encryption protocol. You can configure the encryption protocol after the authentication protocol has been configured. The following table lists the combinations of the authentication protocols and the encryption protocols.

Table 37-5 Combination of the authentication protocol and the encryption protocol

#	Authentication protocol	Encryption protocol
1	None	None
2	MD5 or SHA	None
3	MD5 or SHA	DES

Syntax

To set or change information:

snmp-server user *<user name>* *<group name>* v3 [auth { md5 | sha } *<authentication password>* [priv des *<privacy password>*]]

To delete information:

no snmp-server user *<user name>*

Input mode

`(config)`

Parameters

<user name>

Configures an SNMP security user name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

<group name>

Sets the name of the SNMP security group to which the SNMP security user belongs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

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

auth { md5 | sha } *<authentication password>*

Specifies the authentication protocol and the authentication password.

`md5`: HMAC-MD5 is used for the authentication protocol.

`sha`: HMAC-SHA1 is used for the authentication protocol.

priv des *<privacy password>*

Specifies the encryption protocol and the encryption password.

1. Default value when this parameter is omitted:

   If `auth` and the subsequent portion are omitted, the authenticated received messages and send messages to be authenticated are discarded.

   If `priv des` and the subsequent portion are omitted, the encrypted received messages and send messages to be encrypted are discarded.

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 *Any character string* in *Specifiable values for parameters*.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

snmp-server engineID local

snmp-server view

snmp-server group

snmp-server host

snmp-server view

Sets MIB view information.

The following table lists the number of entries for each parameter that can be set in this command.

Table 37-6 Number of entries for each parameter

#	Parameter	Maximum number of entries
1	MIB view	50 entries per device
2	Subtree	30 entries for a MIB view
3		500 entries per device

Syntax

To set or change information:

snmp-server view *<view name>* *<oid tree>* { included | excluded }

To delete information:

no snmp-server view *<view name>* *<oid tree>*

Input mode

`(config)`

Parameters

<view name>

Sets a MIB view name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see *Any character string* in *Specifiable values for parameters*.

<oid tree>

Sets an object ID that indicates a subtree.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an object ID in dot notation. You can use no more than 64 characters. You can also use a wildcard (`*`) for each sub-ID (numbers separated by a period).

{ included | excluded }

Sets the inclusion or exclusion of a subtree. Specify `included` to include the subtree in the MIB view. Specify `excluded` to exclude the subtree from the MIB view.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify either `included` or `excluded`.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When you change or delete information, if a wildcard (`*`) is specified for a sub-ID for *<oid tree>*, this entry is regarded as the same as the entry for which the sub-ID of the same position is `0`. Also, if you set `0` for a sub-ID, this entry is regarded as the same as the entry for which the sub-ID of the same position is a wildcard (`*`).

   Therefore, if you change information for one entry, information of another entry is also overwritten. If you delete information for one entry, information of another entry is also deleted.

Related commands

snmp-server engineID local

snmp-server user

snmp-server group

snmp-server host

snmp trap link-status

When `no snmp trap link-status` is set, this command prevents a trap (linkDown and linkUp traps) from being sent when a link-up failure or a link-down failure occurs on a line.

Syntax

To set information:

no snmp trap link-status

To delete information:

snmp trap link-status

Input mode

`(config-if)`

Parameters

None

Default behavior

Sending linkDown and linkUp traps is not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

38. Log Data Output Functionality

logging event-kind

Sets the event type of the log information to be sent to the syslog server. Multiple event types can be set.

Syntax

To set or change information:

logging event-kind *<Event kind>*

To delete information:

no logging event-kind *<Event kind>*

Input mode

`(config)`

Parameters

<Event kind>

Specifies the event type of the log information to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `key`, `rsp`, `err`, `evt`, or `aut`.

Default behavior

`evt` or `err` is set as the event type.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The event type set by using this command is applied to all output destinations specified by the `logging host` command.
2. If the event type is set by using this command, the default event types (`evt` and `err`) become invalid and only the event types that have been set take effect.

Related commands

logging host

logging facility

Sets a facility to which log information is output via the syslog interface.

Syntax

To set or change information:

logging facility *<Facility>*

To delete information:

no logging facility

Input mode

`(config)`

Parameters

<Facility>

Specifies the facility for syslog.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify `local0`, `local1`, `local2`, `local3`, `local4`, `local5`, `local6`, or `local7`.

Default behavior

`local0` is used as the facility.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The facility set by using this command is applied to all output destinations specified by the `logging host` command.

Related commands

logging host

logging host

Sets the output destination for log information. The command can configure up to 4 entries.

Syntax

To set or change information:

logging host {*<ipv4 address>* | *<ipv6 address>*} [no-date-info]

To delete information:

no logging host {*<ipv4 address>* | *<ipv6 address>*}

Input mode

`(config)`

Parameters

{ *<ipv4 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:

   <ipv4 address>

   Specifies the IPv4 address in dot notation.

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

   <ipv6 address>

   Specifies the IPv6 address in colon notation.

   ::2 to fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff , fec0:: to feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

no-date-info

Sends the information after excluding the time from log information. If the log type is `EVT` or `ERR`, the information after excluding the time, message ID, and additional information is sent.

For details about the log information format, see *1.2.3 Format of operation logs* in the manual *Message and Log Reference*.

1. Default value when this parameter is omitted:

   All log information is sent.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To use the syslog functionality, a syslog daemon program must be running on the destination host and the host must be configured so that it can receive the syslog information from the Switch.
2. If a large amount of log information is generated at one time, some information might be missing from the syslog information.
3. Even if `no-date-info` is specified, time information remains in the log information saved in the device.
4. 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 functionality adds time information to the message header, the date and time when the log information was sent are displayed in the message at the log output destination.

Related commands

None

logging syslog-dump

When `no logging syslog-dump` is set, this command configures the settings so that log data generated on the switch is not stored in the internal flash memory.

Syntax

To set information:

no logging syslog-dump

To delete information:

logging syslog-dump

Input mode

`(config)`

Parameters

None

Default behavior

Log data is stored in the internal flash memory.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Log indicates the operation log or the reference 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. Executing the `clear logging` operation command accesses the internal flash memory and erases the log data.

Related commands

logging host

logging trap

Sets the level of importance for log information to be sent to the syslog server.

Syntax

To set or change information:

logging trap { *<Level>* | *<Keyword>* }

To delete information:

no logging trap

Input mode

`(config)`

Parameters

{ *<Level>* | *<Keyword>* }

Select either a level or a keyword as the priority of syslog messages.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   The following table describes the priorities that can be set. Note that if a level is specified, information is displayed with the keyword.

Table 38-1 Priorities that can be specified

Level	Keyword	Description
0	emergencies	System unavailable
1	alerts	Immediate action required
2	critical	Critical state
3	errors	Error state
4	warnings	Warning state
5	notifications	Normal but attention required
6	information	Message reporting information
7	debugging	Message displayed during debugging only

Default behavior

`information` (priority level 6) is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The severity set by using this command is applied to all output destinations specified by the `logging host` command.

Related commands

logging host

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 number 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 *Extended data format* in the *Configuration Guide Vol. 2*.

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.

gateway

Enables the sending of gateway information.

user

Enables the sending of user information.

url

Enables the sending of URL information.

none

No flow samples in any extended data format are to be sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   switch, router, gateway, user, url, none

Default behavior

Flow samples in any extended data format are sent to the collector.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Any new setting of this command overwrites the old setting. If you want to change a parameter, enter all the necessary parameter values at the same time when you set this command.
2. The Switch is Layer 2 Switch, which supports neither the transmission of the router information nor the gateway information.

Related commands

None

sflow forward egress

Causes the send traffic of the specified port to be monitored by the sFlow statistics.

Syntax

To set information:

sflow forward egress

To delete information:

no sflow forward egress

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can specify either `sflow forward egress` or `sflow forward ingress` for the switch. To specify the sent traffic as the monitoring target, delete any `sflow forward ingress` command set for other ports, and then set `sflow forward egress` for the port to be monitored.
2. You cannot set this command for the AX2530S-48T and AX2530S-48T2X series switches.

Related commands

sflow forward ingress

sflow forward ingress

Causes the received traffic of the specified port to be monitored by the sFlow statistics.

Syntax

To set information:

sflow forward ingress

To delete information:

no sflow forward ingress

Input mode

`(config-if)`

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can specify either `sflow forward ingress` or `sflow forward egress` for the switch. To specify the received traffic as the monitoring target, delete any `sflow forward egress` command set for other ports, sand then set `sflow forward ingress` for the port to be monitored.

Related commands

sflow forward egress

sflow max-header-size

If the header type is used for the basic data format (see the `sflow packet-information-type` command), sets the maximum size from the beginning of the sample packet to be copied.

Syntax

To set or change information:

sflow max-header-size *<bytes>*

To delete information:

no sflow max-header-size

Input mode

`(config)`

Parameters

<bytes>

If the header type is used for the basic data format, this parameter sets the maximum size to be copied (in bytes), starting from the beginning of the sample packet.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 256

Default behavior

A maximum of 128 bytes are copied from the beginning of the sample packet.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow max-packet-size

Specifies the maximum size of an sFlow packet.

Syntax

To set or change information:

sflow max-packet-size *<bytes>*

To delete information:

no sflow max-packet-size

Input mode

`(config)`

Parameters

<bytes>

Specifies the maximum size of an sFlow packet (in bytes). Specify a value equal to or smaller than the MTU length value (in bytes) 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 *Basic data format* in the *Configuration Guide Vol. 2*.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   ip

Default behavior

Flow samples are sent to the collector in header type format.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow polling-interval

Specifies the interval for sending counter samples to the collector.

Syntax

To set or change information:

sflow polling-interval *<seconds>*

To delete information:

no sflow polling-interval

Input mode

`(config)`

Parameters

<seconds>

Specifies the interval for sending counter samples to the collector (in seconds). If 0 second is specified, counter samples are not sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 2147483647 (=2^{31} - 1)

Default behavior

Counter samples are sent to the collector in every 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If 20 or more ports are monitored, the load on the Switch might be excessive. In such a case, as the guideline, specify an interval value (in seconds) equal to the total number of monitored physical ports.

   Example: If there are 40 monitored physical ports, specify 40 seconds or more for the interval value.

Related commands

None

sflow sample

Specifies the sampling interval applying to the Switch.

Syntax

To set or change information:

sflow sample *<sample count>*

To delete information:

no sflow sample

Input mode

`(config)`

Parameters

<sample count>

Specifies the sampling interval (in the unit of packets) that applies to the Switch. The sampling probability is one packet (sampled) per sampling interval. For example, if the sampling interval is set to 512, the probability of a packet being sampled is one in 512. Use the `show interfaces` operation command to check all the received and sent PPS (number of packets per second) information from the operating status of the port for which sFlow statistics are to be enabled. The recommended value is described in *Table 39-1 Sampling interval to be used as a guideline in an operating environment* in the *Sampling interval to be used as a guideline* column for the applicable total PPS value. If you set a sampling interval that is significantly smaller than the recommended value, the load on the CPU might be excessive.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   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 Sampling interval to be used as a guideline in an operating environment

Total PPS	Sampling interval to be used as a guideline	Example implementation to be used as a guideline
Up to 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

Total PPS	Sampling interval to be used as a guideline	Example implementation to be used as a guideline
Up to 800 kpps	8192	
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

Sampling interval entered in the command	Sampling interval actually set
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 and 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

The source IP address selected by the Switch is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The broadcast address, multicast address, and link-local address cannot be set for the agent IP address of sFlow packets.
2. For the IP address to be used as the agent IP address, specify the IP address assigned to a Switch port. If the specified IP address is not the one set for the Switch, sFlow packets cannot be sent.

Related commands

None

sflow url-port-add

When URL information is used in the extended data format, sets the port number used for HTTP packets to a port number other than 80.

Syntax

To set or change information:

sflow url-port-add *<url port>*

To delete information:

no sflow url-port-add

Input mode

`(config)`

Parameters

<url port>

When URL information is used in the extended data format, sets the port number used for HTTP packets to a port number other than 80.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

The port number used for HTTP packets is set to 80 only.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

sflow version

Sets the version of the sFlow packet to be sent.

Syntax

To set information:

sflow version *<version no.>*

To delete information:

no sflow version

Input mode

`(config)`

Parameters

<version no.>

Sets the version of the sFlow packet to be sent. The sFlow packet of the specified version is sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2

Default behavior

The version of the sFlow packet is 4.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

Part 14: Management of Neighboring Device Information

40. 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)
```

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

Sets the time that a neighboring device retains an LLDP frame sent from a Switch.

Syntax

To set or change information:

lldp hold-count *<Count>*

To delete information:

no lldp hold-count

Input mode

`(config)`

Parameters

<Count>

Sets the scaling for the value set by the `lldp interval-time` command as the time that a neighboring device retains the LLDP frame sent from a 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

Sets the transmission interval between LLDP frames sent from a Switch.

Syntax

To set or change information:

lldp interval-time *<Seconds>*

To delete information:

no lldp interval-time

Input mode

`(config)`

Parameters

<Seconds>

Sets the transmission interval between LLDP frames sent from a Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   5 to 32768 (seconds)

Default behavior

30 seconds is used as the sending interval between LLDP frames sent from the Switch.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

lldp run

lldp run

Enables the LLDP functionality.

Syntax

To set information:

```
lldp run
```

To delete information:

```
no lldp run
```

Input mode

`(config)`

Parameters

None

Default behavior

The LLDP functionality is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

Related commands

None

lldp version

Sets the LLDP version for the Switch.

Syntax

To set information:

lldp version { auto | draft | 2005 }

To delete information:

no lldp version

Input mode

`(config-if)`

Parameters

{ auto | draft | 2005 }

Sets the LLDP version for the Switch.

auto

Automatically discovers the version.

draft

Sets the version to IEEE 802.1AB/D6.0 (October 2003).

2005

Sets the version to IEEE 802.1AB-2005.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   auto, draft, or 2005

Default behavior

`auto` 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

lldp run

Part 15: Port Mirroring

41. Port Mirroring

monitor session

Configures the port mirroring functionality.

Syntax

To set or change information:

monitor session *<session no.>* source interface *<interface id list>* [{rx | tx | both}] destination interface *<interface id list>*

To delete information:

no monitor session *<session no.>*

Input mode

`(config)`

Parameters

<session no.>

Specifies a port mirroring session number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1

source interface *<interface id list>*

Specifies a monitor port for port mirroring.

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:

   None

destination interface *<interface id list>*

Specifies a mirror port for port mirroring. Up to 2 ports can be specified for the mirror ports. A port for which Layer 2 information has been set cannot be specified.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

   See *Specifiable values for parameters*.

Default behavior

None

Impact on communication

If a line in use is set as the mirror port, communication is no longer possible on the line. If a line is set 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. Only one combination of monitor port and mirror port can be set at the same time.
2. A port that has already been set as a monitor port cannot be set as a mirror port.
3. Up to 2 mirror ports can be set for a monitor port. You cannot set more than 3 mirror ports.
4. If the number of frames copied by port mirroring exceeds the line bandwidth, the frames are discarded.
5. Regular frames cannot be sent or received on a port that has been set as a mirror port.
6. A port for which Layer 2 information has been set cannot be set as a mirror port. If you use a port for which Layer 2 information has already been set as a mirror port, delete the Layer 2 information of the applicable interface before setting the port as a mirror port.

Related commands

None

Part 16: Configuration Error Messages

42. Error Messages Displayed When Editing the Configuration

42.1 Error messages displayed when editing the configuration

42.1.1 Common

Table 42-1 Common error messages

Message	Description
<Start allocation> can set only 0.	*<Start allocation>* can be set only to 0.
Access denied.	Access was denied.
Ambiguous command.	The command can be interpreted in two or more ways and therefore cannot be identified uniquely.
Ambiguous data.	The data cannot be identified uniquely because it can be interpreted in various ways.
Ambiguous parameter.	The parameter cannot be identified uniquely because it can be interpreted in various ways.
Authorization error.	An authentication error occurred.
Bad command.	The command was not entered correctly.
Bad value.	The value is incorrect.
Cannot change mdix.	The automatic MDIX functionality cannot be set in the SFP port.
Cannot execute.	The command cannot be executed.
Can't execute.	
Cannot register this command in a range mode.	The command cannot be registered in range mode.
Cannot set TOS/Precedence and DSCP at the same time.	`dscp` cannot be set at the same time as `tos` or `precedence`. Set one or the other.
Cannot set Traffic-class and DSCP at the same time.	`traffic-class` and `dscp` cannot be set at the same time. Set one or the other.
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 execute command it because data is not corresponding.	The command cannot be executed because there is no data matched.
Command chaining not allowed.	Chained commands cannot be entered.
Don't specify a *<MSTI ID list>*.	*<MSTI ID list>* is not required.
Event not found.	The event could not be found.

Message	Description
File not found.	The file could not be found.
Illegal combination 'xxx' and 'yyy'.	The *xxx* parameter and the *yyy* parameter cannot be specified concurrently.
Incomplete command.	The command is incomplete.
Inconsistent name.	The name is inconsistent.
Inconsistent value.	The value is inconsistent.
interface: Invalid IPv4 address.	Interface: The IPv4 address is invalid.
interface: Invalid Mask.	Interface: The mask is invalid.
Invalid parameter order.	Parameters are specified in the wrong order.
Invalid parameter.	An entered parameter was invalid.
Invalid parameter 'xxx'.	The *xxx* parameter is invalid.
Invalid value.	The entered value is invalid.
It will be logged out if it remains idle for another *<min>* minutes.	You will be logged out if the idle state continues for *<min>* more minutes.
Log out by the system.	You have been logged out by the system.
Login incorrect.	You are not permitted to log in to the specified host.
Maximum number of entries are already defined.	The maximum number that has been set has been exceeded. Delete unnecessary entries.
Missing parameter.	A parameter is missing.
Missing parameter data.	Parameter data is missing.
No Access.	Access is not provided.
No help available.	The Help file is invalid.
'no' is not applicable.	no cannot be entered.
No such name.	No such name was found.
Not found:	The item could not be found.
Not writable.	Writing is not possible.
Out of range. Valid range is: *<range>*	The value is not in the specifiable range. The valid range is *<range>*.
Please set parameter more than one.	No parameters have been set.
Read only.	This information is read only.

Message	Description
Resource unavailable.	The resource is invalid.
Some parameters are insufficient.	Some parameters are missing.
String must be more than 0 characters.	A string must have at least one character.
String too long.	The character string is too long.
The command execution failed, because "xxx" is executing.	The command or functionality is being executed by *xxx*. Wait a while and then try again, or else check whether another user is running the command or functionality. Use the `show conf-lock-status` or `who` operation command to check the status.
The different name is already defined.	A different name is already set.
The number of the *<HEX enum>* exceeds a maximum number.	The number of *<HEX enum>* parameters exceeds the maximum.
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 command is not supported with this model.	The command is not supported by this model.
This command uses the "no" prefix.	The command uses the "no" prefix.
Too big.	The value is too large.
Too many parameters.	There are too many parameters.
Unknown user.	The specified user name is not registered.
Wrong encoding.	The encoding method is incorrect.
Wrong length.	The length is incorrect.
Wrong type.	The type is incorrect.
Wrong value.	The value is incorrect.

42.1.2 Login security and RADIUS

Table 42-2 Error messages related to login security and RADIUS

Message	Description
Can't delete it because data is not corresponding.	The specified configuration cannot be deleted because it does not exist.
<Group name> is not available.	The specified RADIUS server group name cannot be set. *<Group name>*: RADIUS server group name

Message	Description
radius-server: Cannot add new group because the maximum number is already set.	No more entries can be registered because maximum number of entries are registered.
radius-server: Cannot add new radius-server host because the maximum number is already set.	No more entries can be registered because maximum number of entries are registered.
radius-server: Port Number is duplicate between auth port and acct port.	The port numbers for `auth-port` and `acct-port` are the same.

42.1.3 Time settings and NTP information

Table 42-3 Error messages related to time settings and NTP

Message	Description
Entry count over	No more NTP server addresses can be set. Check the NTP server addresses that have already been set.

42.1.4 Power saving functionality information

Table 42-4 Error messages related to the power saving functionality

Message	Description
Can't delete system-sleep configuration referred by wakeup-option.	The `schedule-power-control system-sleep` command cannot be deleted because it is used by the `schedule-power-control wakeup-option` command.
Can't execute.	The command could not be executed. Re-execute the command.
Can't set interface, because invalid pair.	The combination of the specified interfaces cannot be set in the WOL packet reception port.
Can't set wakeup-option configuration, because system-sleep isn't setting.	The `schedule-power-control wakeup-option` command cannot be set because the `schedule-power-control system-sleep` command has not been set.
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
Invalid interface.	The specified interface cannot be set in the WOL packet reception port.
Invalid time-range.	An end date that is earlier than the start data is specified. Review Revise the setting.

42.1.5 Ethernet information

Table 42-5 Ethernet error messages

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
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 set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
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.

42.1.6 Link aggregation information

Table 42-6 Link aggregation error messages

Message	Description
Can't delete port-channel configuration referred by other configuration.	The VLAN cannot be deleted because it is being used by another configuration.
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.
dot1x(link-aggregation): The specified ethernet *<IF#>* cannot add to the specified port-channel(*<Channel group#>*) because 802.1X configuration is different.	`ethernet` *<IF#>* cannot be registered in `port-channel` *(<Channel group#>)* that has been specified because the IEEE 802.1X configuration, which must be consistent within the link aggregation, is different. *<IF#>*: Interface port number *<Channel group#>*: Channel group number
interface : 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.
interface : 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.
interface : 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
interface : Invalid authentication arp-relay configuration.	Participation in the port channel is not possible because the `authentication arp-relay` setting is different.
interface : Invalid authentication ip access-group configuration.	Participation in the port channel is not possible because the `authentication ip access-group` setting is different.
interface : This command is different from authentication configuration in channel-group port.	Participation in the port channel is not possible because the configuration common to all authentication modes is different.
interface : This command is different from the mac-authentication configuration in the channel-group port.	Participation in the port channel is not possible because the MAC-based authentication configuration is different.
interface : This command is different from the web-authentication configuration in the channel-group port.	Participation in the port channel is not possible because the Web-based authentication configuration is different.
interface : this command is different from this one in channel-group port.	Participation in the port channel is not possible because the configuration is different.
invalid data[channel-group].	The specified port channel number is invalid.
invalid data[ethernet-if].	The specified interface port number is invalid.
Maximum number of channel-group port are already defined.	No more ports can be set. Check the number of ports for each channel group.
Mirror port and port-channel are inconsistent.	The port cannot join the port channel because the port is being used as a mirror port.
Relations between ip dhcp snooping configuration and channel-group configuration are inconsistent.	The specified port cannot join the port channel because the port is being used by the `ip dhcp snooping` configuration. Delete the setting of `ip dhcp snooping`, and then set it again.
Relations between ip source binding configuration and channel-group configuration are inconsistent.	The specified port cannot join the port channel because the port is being used by the `ip source binding` configuration. Delete the `ip source binding` setting, and then set it again.
	The specified port cannot be deleted because it is being used by the `ip source binding` configuration. Delete the `ip source binding` setting, and then set it again.
Relations between ip verify source configuration and channel-group configuration are inconsistent.	The specified port cannot join the port channel because the port is being used by the `ip verify source` configuration. Delete the `ip verify source` setting, and then set it again.
Relations between vlan in mac-address-table static configuration and channel-group configuration are inconsistent.	The interface cannot join the port channel because the interface is being used by the `mac-address-table static` configuration.

Message	Description
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.
vlan : Data(port-channel) is invalid.	The specified port channel number is invalid.
vlan : This command is different from vlan configuration in channel-group port.	The VLAN cannot join the port channel because the VLAN configuration is different.
web-auth : Cannot set the command because of internal error. (code=x)	The command could not be set because an internal error has occurred.

42.1.7 MAC address table information

Table 42-7 MAC address table error messages

Message	Description
Can't set mac-address-table because of port-channel nothing.	mac-address-table cannot be set because there is no port channel.
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
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 set by switchport access/switchport trunk allowed vlan/switchport mac vlan/switchport protocol vlan of the interface that has been set.

42.1.8 VLAN information

Table 42-8 VLAN error messages

Message	Description
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 set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
ChGr *<Channel group#>*: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	The port channel cannot be deleted because it is being used for IEEE 802.1X authentication or as a switch port. *<Channel group#>*: Channel group number
Duplicate translated id.	The value of the specified VLAN tag is being used for other VLAN.

Message	Description
interface : Relations between the mac-authentication configuration and the vlan mode configuration are inconsistent.	The configuration of the specified port cannot be changed because the port is being used for MAC-based authentication. Delete the `mac-authentication port` configuration, and then reconfigure.
interface : Relations between the web-authentication configuration and the vlan mode configuration are inconsistent.	The configuration of the specified port cannot be changed because the port is used for Web authentication. Delete the `web-authentication port` configuration, and then reconfigure.
interface : VLAN is not Port VLAN.	The specified VLAN is not a port VLAN. Specify a port VLAN.
interface : VLAN is not Port VLAN or MAC VLAN.	The specified VLAN is not port VLAN or MAC VLAN. Specify port VLAN or MAC VLAN.
Mirror port and switchport are inconsistent.	Both mirror port and switch port settings cannot be specified simultaneously.
Not found *<VLAN ID>*.	The specified VLAN ID cannot be set. *<VLAN ID>*: VLAN ID
port *<IF#>*: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	The configuration of the specified port cannot be changed because the port is being used for IEEE 802.1X authentication. *<IF#>*: Interface port number
Relations between access-list and dot1q-tunnel are inconsistent.	If VLAN tunneling is set, the access list cannot be applied to the sending side of the VLAN interface. Also, VLAN conditions cannot be specified as the filter conditions of the access list that is applied to the sending side of the Ethernet interface.
Relations between access-list and vlan mapping are inconsistent.	If tag translation is set, the access list cannot be applied to the sending side of the VLAN interface. Also, VLAN conditions cannot be specified as the filter conditions of the access list that is applied to the sending side of the Ethernet interface.
Relations between dot1q ethertype and sml configuration are inconsistent.	A command that affects TPID of the SML peer link cannot be specified.
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 functionality is set.
Relations between igmp snooping and vlan-tunneling are inconsistent.	The IGMP snooping functionality and VLAN tunneling cannot be specified concurrently.
Relations between ip dhcp snooping configuration and vlan mapping configuration are inconsistent.	vlan mapping cannot be specified for a trunk port in a VLAN for which `ip dhcp snooping vlan` is set.
Relations between ip dhcp snooping configuration and vlan-tunneling configuration are inconsistent.	`ip dhcp snooping vlan` and VLAN tunneling cannot be specified concurrently.

Message	Description
Relations between mac-based and vlan-tunneling-enable are inconsistent.	MAC VLANs and VLAN tunneling cannot be set concurrently.
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 functionality is set.
Relations between mld snooping and vlan-tunneling are inconsistent.	The MLD snooping functionality and VLAN tunneling cannot be specified concurrently.
Relations between protocol-based and vlan-tunneling-enable are inconsistent.	A protocol VLAN and VLAN tunneling cannot be set concurrently.
Relations between the dot1x configuration and the VLAN mode configuration are inconsistent.	Port-based authentication cannot be set for a port whose VLAN mode is tunneling mode.
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 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 protocolVLAN mode.
Relations between vlan in access-group configuration and switchport configuration are inconsistent.	The configuration of the specified VLAN cannot be changed because the VLAN is being used by `ip access-group` or `mac access-group`. Delete the configuration of `ip access-group` or `mac access-group` for the applicable VLAN, and then reconfigure.
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 set because they set the same VLAN.
Relations between vlan in ip source binding configuration and switchport configuration are inconsistent.	The configurations cannot be changed because `ip source binding` is using it. Delete the `ip source binding` setting, and then set it again.
Relations between vlan in qos-flow-group configuration and switchport configuration are inconsistent.	The configuration of the specified VLAN cannot be changed because it is used by `ip qos-flow-group` or `mac qos-flow-group`. Delete the configuration of `ip qos-flow-group` or `mac qos-flow-group` for which the applicable VLAN is set, and then reconfigure.
Relations between vlan-mapping and dot1q ethertype configuration are inconsistent.	Tag translation and TPID cannot be specified concurrently.

Message	Description
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.
vlan : Can't change mode from {nothing|protocol-based|mac-based } to {nothing|protocol-based|mac-based }.	The VLAN types of the specified VLAN modes do not match (VLAN range specification).
vlan : Can't delete vlan configuration because of default vlan.	The VLAN cannot be deleted because it is the default VLAN.
vlan : Can't setting port[*<IF#>*] because of channel-group port.	The specified port number cannot be set from the port because the port number belongs to the channel group. *<IF#>*: Interface port number
vlan : Data(mac-address) is invalid.	The specified `mac-address` cannot be registered because it is not in the specifiable range.
vlan : maximum number which can be used is exceeded.	No more entries can be generated because the number of VLANs exceeds the maximum number of entries.
vlan : Not found protocol name.	The VLAN cannot be set because `vlan-protocol` has not been set.
vlan : Some port's setting have been failed.	Setting of a port from a channel has failed.
vlan : Some setting can't have been done because of vlan unmatch.	Some VLANs cannot be set because at least one of the VLANs does not exist.
vlan[*<VLAN ID>*] : Can't change mode from {nothing|protocol-based|mac-based} to {nothing|protocol-based|mac-based}.	The VLAN types of the specified VLAN modes do not match. (Only VLAN is specified.) *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Can't delete it because data is not corresponding.	The specified VLAN cannot be deleted because it does not exist. The specified `mac-address` cannot be deleted because it is not registered. The specified `mac-address-table` cannot be deleted because it does not exist. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Can't delete port-channel configuration referred by other configuration.	The VLAN cannot be deleted because it is being used by another configuration. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Can't delete vlan configuration referred by other configuration.	The VLAN cannot be deleted because it is being used by another configuration. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Can't set access vlan which is not configured to use vlan.	The access VLAN cannot be set because the VLAN does not exist. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Can't set mac-address-table static which is not configured to use vlan.	`mac-address-table` cannot be set because the VLAN does not exist.

Message	Description
	<VLAN ID>: VLAN ID
vlan[*<VLAN ID>*] : Can't set native vlan which is not configured to use vlan.	The native VLAN cannot be set because the VLAN does not exist. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Data can't be set because of not mac-based.	`mac-address` cannot be registered because the specified VLAN is not a MAC VLAN. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Data can't be set because of not protocol-based.	`protocol` cannot be registered because the specified VLAN is not a protocol VLAN. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : mac-address has already been set to other VLAN[*<VLAN ID>*].	The `mac-address` cannot be registered because it has already been registered for another VLAN. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : maximum number which can be used is exceeded.	No more entries can be generated because the number of VLANs exceeds the maximum number of entries. No more VLANs can be registered because the number of registered `mac-address` items exceeds the maximum number of entries. No more entries can be registered because the number of registered `mac-address-table` items exceeds the maximum number of entries. *<VLAN ID>*: VLAN ID
vlan[*<VLAN ID>*] : Protocol {ethertype|llc|snap-ethertype} *<HEX>* duplicate at ChGr[*<Channel group#>*].	Only one VLAN to be specified by the same protocol value can be set on the same port channel. *<VLAN ID>*: VLAN ID *<HEX>*: Protocol value *<Channel group#>*: Channel group number
vlan[*<VLAN ID>*] : Protocol {ethertype|llc|snap-ethertype} *<HEX>* duplicate at port[*<IF#>*].	Only one VLAN to be specified by the same protocol value can be set on the same port. *<VLAN ID>*: VLAN ID *<HEX>*: Protocol value *<IF#>*: Ethernet port number
vlan-protocol : Cannot delete protocol referred by VLAN configuration.	The protocol cannot be deleted because `protocol` uses it.
vlan-protocol : 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 Switch. No more than 16 VLANs can be set.

42.1.9 Spanning Tree information

Table 42-9 Spanning tree error messages

Message	Description
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
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 entries are already defined. *<STP_VLAN>*	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.
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 l2protocol-tunnel stp and spanning-tree configuration are inconsistent.	The relations between the BPDU forwarding configuration and the Spanning Tree configuration are inconsistent. When a BPDU forwarding configuration is set, the Spanning Tree Protocol must be stopped.
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.
Too many parameters (VLAN-range of MST Instance *<MSTI ID>*).	The number of input parameters exceeds the maximum number (200). Set a value equal to or smaller than the maximum number. *<MSTI ID>*: MST instance ID

42.1.10 Ring Protocol information

Table 42-10 Ring Protocol error messages

Message	Description
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>*: Can't delete axrp configuration referred by other.	The specified ring ID cannot be deleted because it is being used by the `axrp-ring-port` command. *<Ring ID>*: Ring ID

Message	Description
axrp-*<Ring ID>*: maximum number of ring-id are already defined.	The maximum number that has been set has been exceeded. 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
axrp-*<Ring ID>*: Relations between uplink redundant and the Ring Protocol are inconsistent.	The uplink redundant functionality has already been set for the specified interface. Delete the uplink redundancy functionality or specify another interface. *<Ring ID>*: Ring ID
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

Message	**Description**
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
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-*<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-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

Message	Description
	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 functionality has been set.
Cannot configure multi-fault-detection when axrp-virtual-link is configured.	The multi-fault monitoring functionality cannot be set because a virtual link has been set.
Cannot configure when forwarding-delay-time is running.	The configuration cannot be set because `forwarding-delay-time` is in operation.
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.

42.1.11 IGMP snooping information

Table 42-11 IGMP snooping error messages

Message	Description
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
Maximum number of VLAN are already defined, *<VLAN ID>* igmp snooping can not enable.	The maximum number of VLANs that can be specified by using the IGMP snooping functionality is 32. No more than 32 VLANs can be set. *<VLAN ID>*: VLAN ID
Relations between igmp snooping and vlan-tunneling are inconsistent.	The IGMP snooping functionality and VLAN tunneling cannot be specified concurrently.
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 functionality is set.

42.1.12 MLD snooping information

Table 42-12 MLD snooping error messages

Message	Description
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.

Message	Description
Duplicate mld query message source address.	The setting is not possible because the source IP address of the same MLD query message has already been defined.
Maximum number of VLAN are already defined, *<VLAN ID>* mld snooping can not enable.	The maximum number of VLANs that can be specified by using the MLD snooping functionality is 32. No more than 32 VLANs can be set. *<VLAN ID>*: VLAN ID
Relations between ip address and mld snooping source address are inconsistent.	IPv6 functionality enabling setting and source IPv6 address of MLD snooping cannot be concurrently specified in the same VLAN.
Relations between mld snooping and vlan-tunneling are inconsistent.	The MLD snooping functionality and VLAN tunneling cannot be specified concurrently.
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 functionality is set.

42.1.13 IPv4, ARP, and ICMP information

Table 42-13 IPv4, ARP, and ICMP error messages

Message	Description
ip : Inconsistency has occurred in a setting of IP address and ARP.	There is an inconsistency between the network addresses of an address set in the IP information and an address set in the ARP information. Specify the network addresses correctly.
ip : Inconsistency has occurred in a setting of IP address and route.	There is an inconsistency between an address set by using IP information and a next-hop network address set by using routing information. Set the next hop correctly.
ip : IP address is duplicate between interface and ARP entry.	An address set by using IP information and an address set by using ARP information are the same. Set the addresses that do not duplicate one another.
ip : IP address is duplicate between interface and nexthop.	An address set by using IP information and a next-hop address set by using routing information are the same. Set the addresses that do not duplicate one another.
ip : maximum number of route are already defined.	No more routing information can be set. Review the network configuration.
ip : The number of pieces of the ARP entry exceeds the capacity of this system.	The number of ARP table entries exceeds the maximum number of entries of the Switch.
ip[*<VLAN ID>*] : Can't delete a primary IP address when a secondary IP address is existing.	A secondary IP address exists. Delete the secondary IP address, and then delete the primary IP address. *<VLAN ID>*: VLAN ID

Message	Description
ip[*<VLAN ID>*] : Can't delete IP configuration with arp configuration.	ARP information exists. Delete the ARP information, and then delete the IP information. *<VLAN ID>*: VLAN ID
ip[*<VLAN ID>*] : Can't delete IP configuration with dhcp configuration.	The DHCP server setting already exists. Delete the DHCP server setting, and then delete the IP information. *<VLAN ID>*: VLAN ID
ip[*<VLAN ID>*] : Can't delete IP configuration with route configuration.	Routing information exists. Delete the routing information, and then delete the IP information. *<VLAN ID>*: VLAN ID
ip[*<VLAN ID>*] : Can't set a secondary IP address on a interface which does not have a primary IP address.	An attempt is being made to set a secondary IP address on an interface on which a primary IP address is not set. Set a primary IP address first. *<VLAN ID>*: VLAN ID
ip[*<VLAN ID>*] : Duplicate network address.	An IP address of the same network address is defined for another VLAN. Set the IP address so that all network addresses are unique. *<VLAN ID>*: VLAN ID
	An IP address for the same network address is set for the Web authentication IP address. Set the IP address so that it does not duplicate the network address for the Web authentication IP address. *<VLAN ID>*: VLAN ID
ip[*<VLAN ID>*] : Interface not found.	The specified interface cannot be found. Check the interface setting. *<VLAN ID>*: VLAN ID
ip[*<VLAN ID>*] : maximum number of IP configuration are already defined.	No more IP addresses can be set. Review the network configuration. *<VLAN ID>*: VLAN ID

42.1.14 IPv6, NDP, and ICMPv6 information

Table 42-14 IPv6, NDP, and ICMPv6 information error messages

Message	Description
ip : IP address is duplicate between interface and default gateway.	An address set by using IP information and an address set by using default gateway information are the same. Set the addresses that do not duplicate one another.
ip : IP address is duplicate between interface and static NDP entry.	An address set by using IP information and an address set by using NDP information are the same. Set the addresses that do not duplicate one another.
ip : The number of pieces of the NDP entry exceeds the capacity of this	The number of NDP table entries exceeds the maximum number of entries of the Switch.

Message	Description
system.	
ip[<VLAN ID>] : Duplicate prefix.	IP addresses with the same prefix have been set. Make sure that prefixes are unique. <VLAN ID>: VLAN ID
ip[<VLAN ID>] : Interface not found.	The specified interface cannot be found. Check the interface setting. <VLAN ID>: VLAN ID
ip[<VLAN ID>] : Invalid IPv6 address -- <value1>	The IPv6 address or IPv6 link-local address is invalid. Set a correct IPv6 address. <value1>: Invalid value
Relations between ip address and mld snooping source address are inconsistent.	IPv6 functionality enabling setting and source IPv6 address of MLD snooping cannot be concurrently specified in the same VLAN.

42.1.15 DHCP server functionality information

Table 42-15 DHCP server functionality error messages

Message	Description
<Pool name> overlaps with other entries.	`network` and `host/hardware-address` cannot be specified at the same time in the same pool. Delete one of them, and then set the other.
Can not delete it because data is not corresponding.	The specified setting cannot be deleted because it does not exist.
Exceeded the number of maximums that it was managed with IP dhcp pool.	The maximum number of managed subnets was exceeded. Revise the network configuration and the host configuration.
Host is already used.	The host which has the same IP address has already been used. Specify a different IP address.
Interface not found.	No VLANs or IP addresses are set. Revise the VLAN and IP settings.
Invalid network.	The network configuration is invalid.
ip [<VLAN ID>]: Can't delete IP configuration with dhcp configuration.	The IP cannot be deleted or changed because it is being used by the DHCP server configuration. <VLAN ID>: VLAN ID
It exceeded maximum number of IP-address pool.	The maximum number of IP address pools has been exceeded. Revise the network configuration and excluded address settings.
Maximum number of entries are already defined. <DHCP-EXCLUDED-ADDRESS>	The maximum number of specifiable excluded addresses has been exceeded.

Message	Description
Maximum number of entries are already defined. *<DHCP-HOST>*	The maximum number of specifiable static IP addresses has been exceeded.
Maximum number of entries are already defined. *<DHCP-IF>*	The maximum number of specifiable interfaces has been exceeded.
Maximum number of entries are already defined. *<DHCP-POOL>*	The maximum number of specifiable pools has been exceeded.
Maximum number of entries are already defined. *<DHCP_SUBNET>*	The maximum number of specifiable subnets has been exceeded.
network conflicts.	Network settings have been duplicated.
This configuration has already been set.	This configuration has already been set.
vlan [*<VLAN ID>*]: Can't delete vlan configuration referred by other configuration.	The VLAN cannot be deleted because it is being used by the DHCP server configuration. *<VLAN ID>*: VLAN ID

42.1.16 Flow detection mode information

Table 42-16 Flow mode error messages

Message	Description
Cannot change the flow detection mode.	The flow detection mode cannot be changed because the receiving side of an access list or a QoS flow list is applied to the interface. To change the flow detection mode, delete all uses of the applied lists.
Cannot change the flow detection out mode.	The flow detection mode cannot be changed because the sending side of an access list or a QoS flow list is applied to the interface. To change the flow detection mode, delete all uses of the applied lists.

42.1.17 Access list information

Table 42-17 Access list error messages

Message	Description
Cannot attach this list because flow detection mode layer2-1.	If the flow detection mode is layer2-1, the access list cannot be applied. If the flow detection mode is layer2-1, a MAC access list can be applied. To do so, you can use the following command: `mac access-group` command

Message	Description
Cannot attach this list because flow detection mode layer2-2.	If the flow detection mode is layer2-2, the access list cannot be applied. If the flow detection mode is layer2-2, an IPv4 access list can be applied. To do so, you can use the following command: `ip access-group` command
Cannot attach this list because flow detection mode layer2-3.	If the flow detection mode is layer2-3, the access list cannot be applied. If the flow detection mode is layer2-3, IPv4 and IPv6 access lists can be applied. To do so, you can use the following command: `ip access-group` command `ipv6 traffic-filter` command
Cannot attach this list because flow detection out mode layer2-1-out.	If the flow detection mode is layer2-1-out, the access list cannot be applied. If the flow detection mode is layer2-1-out, a MAC access list can be applied. To do so, you can use the following command: `mac access-group` command
Cannot attach this list because flow detection out mode layer2-2-out.	If the flow detection mode is layer2-2-out, the access list cannot be applied. If the flow detection mode is layer2-2-out, an IPv4 access list can be applied. To do so, you can use the following command: `ip access-group` command
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.
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.	If VLAN tunneling is set, the access list cannot be applied to the sending side of the VLAN interface. Also, VLAN conditions cannot be specified as the filter conditions of the access list that is applied to the sending side of the Ethernet interface.
Relations between access-list and vlan mapping are inconsistent.	If tag translation is set, the access list cannot be applied to the sending side of the VLAN interface. Also, VLAN conditions cannot be specified as the filter conditions of the access list that is applied to the sending side of the Ethernet interface.
The maximum number of TCP/UDP port entries are exceeded.	The number of entries used to specify the range of TCP/UDP port numbers exceeds the maximum. The entries for specifying a range of TCP/UDP port numbers include up to 16 patterns.

Message	Description
	The number of used entries and available entries in the configuration file can be checked by using the show system operation command.
This list cannot be set for out.	This access list cannot be applied to the sending-side flow detection mode. If the class is set as a flow detection condition in an access list, the access list cannot be applied to the sending-side flow detection mode.
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 command: ip access-group command ipv6 traffic-filter command
The sequence number exceeded the maximum value. Try "resequence" Command.	The automatic sequence number exceeds the maximum value. Execute the resequence command.
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.
This list name is being used as other protocol type by other definition.	The identifier cannot be set because it is a name that has already been used for another access list. Specify a name that is not being used for another access list.
The maximum number of entries are exceeded.	The number of specifiable entries was exceeded. Delete unnecessary entries before executing the command.

42.1.18 QoS information

Table 42-18 QoS error messages

Message	Description
Can not set command, because limit-queue-length command is set.	A scheduling mode other than PQ cannot be set because the limit-queue-length command is set.
Can not set command, because scheduling modes is not PQ.	The limit-queue-length command cannot be set because a scheduling mode other than PQ is set.

Message	Description
Can not set half duplex because traffic-shape rate is specified for the port.	Duplex mode cannot be set because port bandwidth control is set for the line.
Can not set half duplex because WFQ min-rate is specified for the port.	Duplex mode cannot be set because the minimum guaranteed bandwidth of WFQ mode is set for the line.
Can not set traffic-shape rate because of the port is half duplex.	Port bandwidth control cannot be set because the line is half duplex.
Can not set WFQ min-rate because of the port is half duplex.	The minimum guaranteed bandwidth of WFQ mode cannot be set because the line is half duplex.
Cannot attach this list because flow detection mode layer2-1.	If the flow detection mode is layer2-1, the QoS flow list cannot be applied. If the flow detection mode is layer2-1, a MAC QoS flow list can be applied. To do so, you can use the following command: `mac qos-flow-group` command
Cannot attach this list because flow detection mode layer2-2.	If the flow detection mode is layer2-2, the QoS flow list cannot be applied. If the flow detection mode is layer2-2, an IPv4 QoS flow list can be applied. To do so, you can use the following command: `ip qos-flow-group` command
Cannot attach this list because flow detection mode layer2-3.	If the flow detection mode is layer2-3, the QoS flow list cannot be applied. If the flow detection mode is `layer2-3`, IPv4 QoS and IPv6 QoS flow lists can be applied. To do so, you can use the following command: `ip qos-flow-group` command `ipv6 qos-flow-group` command
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.
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.
The maximum number of TCP/UDP port entries are exceeded.	The number of entries used to specify the range of TCP/UDP port numbers exceeds the maximum. The entries for specifying a range of TCP/UDP port numbers include up to 16 patterns. The number of used entries and available entries in the configuration file can be checked by using the `show system` operation command.
The different name is already defined.	An entry cannot be added to an interface for which queue group has already been set.

Message	Description
The Maximum number of entries are already defined. *<QOSFLOW_GROUP>*	The maximum number of applications to a QoS flow list interface has been exceeded.
The Maximum number of entries are already defined. *<QOSFLOW_LIST>*	The maximum number of QoS flow list remark settings has been exceeded.
The Maximum number of entries are already defined. *<QOSFLOW_MAC>*	The number of entries for a MAC-QoS flow list exceeds the capacity limit.
The maximum number of entries are exceeded.	The number of QoS entries exceeds the capacity limit. The number of used entries and available entries in the configuration can be checked by using the `show system` command.
The sequence number exceeded the maximum value. Try "resequence" Command.	The automatic sequence number has exceeded the maximum value. Execute the `resequence` command.
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.
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.

42.1.19 Layer 2 authentication common information

Table 42-19 Error messages common to Layer 2 authentication

Message	Description
interface : Invalid access-list ID for authentication.	The access list is different from the one that has already been applied by using `authentication ip access-group` (only one list name can be applied).) Set an access list that has already been set. Alternatively, delete all access lists that have already been applied to another interface, and then set this again.

Message	Description
interface : Invalid authentication arp-relay configuration.	authentication arp-relay cannot be set because none of the following commands are set for the applicable port: ● dot1x port-control ● web-authentication port ● mac-authentication port Set any of the above commands for the applicable port, and then set authentication arp-relay again.
interface : Invalid authentication ip access-group configuration.	authentication ip access-group cannot be set because none of the following commands are set for the applicable port: ● dot1x port-control ● web-authentication port ● mac-authentication port Set any of the above commands for the applicable port, and then set authentication ip access-group again.
interface : Over two entry as an address family cannot be set.	Another access list has already been applied. Delete an existing access list, and then set this again.
interface : Relations between authentication configuration and channel-group configuration are inconsistent.	The applicable port cannot be set because it belongs to a channel group. Sets up a port channel interface.
interface : Relations between the switchport mac vlan and authentication force-authorized vlan are inconsistent.	authentication force-authorized vlan cannot be set because the specified VLAN is not a MAC VLAN.
max-user: Cannot set the command because of internal error. (code=x)	The command could not be set because an internal error has occurred. x : 1, 2

42.1.20 IEEE 802.1X information

Table 42-20 IEEE 802.1X error messages

Message	Description
dot1x(xxxxx): Cannot set "dot1x port-control" because monitor session mode is set now.	Port-based authentication cannot be set because port mirroring of the *xxxxx* interface is enabled. *xxxxx*: ethernet *<IF#>*: Ethernet interface port number
dot1x(xxxxx): Cannot set " dot1x authentication " command because user-group configuration is set now.	The dot1x authentication command cannot be set because the user ID-based authentication method is enabled on the *xxxxx* interface. Delete the settings of the web-authentication user-group command. *xxxxx*: ethernet *<IF#>*: Ethernet interface port number port-channel *<Channel group#>*: Port channel number

Message	Description
dot1x(link-aggregation): Cannot set the configuration because the ethernet *<IF#>* belongs to the port-channel	IEEE 802.1X cannot be set because the specified `ethernet` *<IF#>* belongs to the port channel. *<IF#>*: Interface port number
dot1x(xxxx): Cannot delete "dot1x port-control" because authentication ip access-group/arp-relay is set.	`dot1x port-control` cannot be deleted because `authentication arp-relay` and `authentication ip access-group` are set for the *xxxxx* interface. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx): Cannot set "dot1x ignore-eapol-start" because reauthentication mode is invalid.	The functionality for suppressing the re-authentication of requests from a terminal cannot be set because the re-authentication request functionality of the *xxxxx* interface is not enabled. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx): Cannot set "dot1x ignore-eapol-start" because supplicant-detection is disable-method.	The functionality for suppressing the re-authentication of requests from a terminal cannot be set because the terminal detection mode of the *xxxxx* interface is disabled. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x: Cannot set "aaa authentication dot1x" because the maximum number is already set.	No more entries can be registered because the maximum number of entries are already registered in the authentication method list.
dot1x(xxxxx): Cannot set "dot1x multiple-authentication" because force-mode is set now.	Terminal authentication mode cannot be set because the *xxxxx* interface is in force-unauthorized mode or force-authorized mode. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx): Cannot set "dot1x port-control force" command because sub-mode is multiple-authentication.	`force-unauthorized` or `force-authorized` mode cannot be set because the *xxxxx* interface is in terminal authentication mode. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx): Cannot set "dot1x port-control" because switchport mode is not access-mode.	Port-based authentication cannot be set because the switch port mode of the *xxxxx* interface is neither access mode nor MAC VLAN. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx):Cannot set "dot1x port-control force" because switchport mode is mac-vlan mode.	Force-unauthorized or force-authorized mode cannot be set because the switch port mode of the *xxxxx* interface (`ethernet` *<IF#>* or `port-channel` *<Channel group#>*) is mac-vlan mode. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number

Message	Description
	`port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx):Cannot set "dot1x port-control" because of a wrong "switchport mode".	IEEE 802.1X authentication cannot be set because switchport mode of interface *xxxxx* (*ethernet <IF#>* or *port-channel <Channel group#>*) is inappropriate. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx): Cannot set "dot1x supplicant-detection disable" because ignore-eapol-start is set now.	Terminal detection mode cannot be disabled because the functionality for suppressing the re-authentication of requests from a terminal on the *xxxxx* interface is set. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x(xxxxx): Cannot set "no dot1x reauthentication" because ignore-eapol-start is set now.	The re-authentication request functionality cannot be disabled because the functionality for suppressing the re-authentication of requests from a terminal on the *xxxxx* interface is set. *xxxxx*: `ethernet` *<IF#>*: Ethernet interface port number `port-channel` *<Channel group#>*: Port channel number
dot1x: Cannot set "dot1x system-auth-control" because l2protocol-tunnel eap configuration is valid now.	IEEE 802.1X cannot be set because the EAPOL forwarding functionality is enabled.
l2protocol-tunnel: Cannot set "l2protocol-tunnel eap" because 802.1X configuration is valid now.	The EAPOL forwarding functionality cannot be set because IEEE 802.1X is enabled.
radius-server: Cannot add new radius-server host because the maximum number is already set.	No more entries can be registered because maximum number of entries are registered.
radius-server: Port Number is duplicate between auth port and acct port.	The port numbers for `auth-port` and `acct-port` are the same.
Relations between the dot1x configuration and the VLAN mode configuration are inconsistent.	Port-based authentication cannot be set for a port whose VLAN mode is tunneling mode.
xxxxx: Cannot set the command because of internal error. (code=y)	The command could not be set because an internal error has occurred. *xxxxx*: dot1x / radius-server / l2protocol-tunnel, *y*: 1, 2, 3, 4

42.1.21 Web authentication information

Table 42-21 Web authentication error messages

Message	Description
Conflicting port number.	The same Web authentication port number is used more than once. Eliminate duplication of Web authentication port numbers.
Duplicate network address.	An IP address of the same network address is defined for another VLAN. Set the Web authentication IP address so that it does not duplicate a VLAN network address.
interface : Invalid web-authentication port configuration.	The `web-authentication port` command cannot be deleted because the following commands are set on the applicable port: ● authentication ip access-group ● authentication arp-relay
interface : Relations between the web-authentication configuration and the channel-group configuration are inconsistent.	The applicable port cannot be set because it belongs to a channel group. Sets up a port channel interface.
interface : Relations between the web-authentication configuration and the vlan mode configuration are inconsistent.	Web authentication cannot be set because the specified port has been set as a tunneling port or a protocol port.
interface : Relations between the web-authentication configuration and the mirror configuration are inconsistent.	Web authentication cannot be set because the specified port has been set as a mirror port.
interface : Relations between user-group configuration and authentication list configuration(s) are inconsistent.	The `web-authentication authentication` command cannot be set because the user ID-based authentication method is set. Delete the settings of the `web-authentication user-group` command.
radius-server: Cannot add new radius-server host because the maximum number is already set.	No more entries can be registered because maximum number of entries are registered.
radius-server: Port Number is duplicate between auth port and acct port.	The port numbers for `auth-port` and `acct-port` are the same.
web-auth : Cannot set the command because of internal error. (code=x)	The command could not be set because an internal error has occurred.
web-auth : Maximum number of entries are already defined. *<LIST-NAME>*	The maximum number of entries for the authentication method list has been exceeded.
web-auth : Relations between authentication list configuration(s) and user-group configuration are inconsistent.	The `web-authentication user-group` command cannot be set because the port-based authentication method is set. Delete the following: ● dot1x authentication ● web-authentication authentication ● mac-authentication authentication

42.1.22 MAC-based authentication information

Table 42-22 MAC-based authentication error messages

Message	Description
interface : Invalid mac-authentication port configuration.	Deletion is not possible because `authentication ip access-group` or `authentication arp-relay` is set for the applicable port.
interface : Relations between the mac-authentication configuration and the channel-group configuration are inconsistent.	The applicable port cannot be set because it belongs to a channel group. Sets up a port channel interface.
interface : Relations between the mac-authentication configuration and the vlan mode configuration are inconsistent.	MAC-based authentication cannot be set because the specified port has been set as a tunneling port or a protocol port.
interface : Relations between the mac-authentication configuration and the mirror configuration are inconsistent.	MAC-based authentication cannot be set because the specified port has been set as a mirror port.
interface : Relations between user-group configuration and authentication list configuration(s) are inconsistent.	The `mac-authentication authentication` command cannot be set because the user ID-based authentication method is set. Delete the settings of the `web-authentication user-group` command.
mac-auth : Cannot set the command because of internal error. (code=x)	The command cannot be set because an internal error occurred.
mac-auth : Maximum number of entries are already defined. *<LIST-NAME>*	The maximum number of entries for the authentication method list has been exceeded.
radius-server: Cannot add new radius-server host because the maximum number is already set.	No more entries can be registered because maximum number of entries are registered.
radius-server: Port Number is duplicate between auth port and acct port.	The port numbers for `auth-port` and `acct-port` are the same.

42.1.23 Multistep authentication information

Table 42-23 Multistep authentication error messages

Message	Description
interface : Relations between authentication configuration and channel-group configuration are inconsistent.	The applicable port cannot be set because it belongs to a channel group. Sets up a port channel interface.
multi-step: Cannot set the command because of internal error. (code=x)	The command could not be set because an internal error has occurred. x : 1, 2

42.1.24 DHCP snooping information

Table 42-24 DHCP snooping error messages

Message	Description
Can't delete it because data is not corresponding.	Deletion is not possible because DHCP snooping for the specified VLAN is not enabled or the specified configuration does not exist.
Can't delete it vlan configuration referred by other configuration.	Deletion is not possible because the `ip source binding` setting uses the VLAN. First, delete the `ip source binding` setting that specifies the VLAN you want to delete.
Can't set it because snooping is disable.	The specified VLAN cannot be set because DHCP snooping for the VLAN is not enabled. Specify a VLAN for which DHCP snooping is enabled.
Can't set it because there are a lot of entries in mac-vlan.	DHCP snooping cannot be set because more than 500 terminals in MAC VLAN have been registered. After reducing the number of terminals in MAC VLAN to 500 or less, set DCHP snooping.
Can't set it because vlan doesn't exist.	The VLAN specified by using `no ip dhcp snooping vlan` cannot be deleted because it does not exist.
	The VLAN specified by using `no ip arp inspection vlan` cannot be deleted because it does not exist.
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
Duplicate entry.	The setting is not possible because the setting duplicates another setting. Delete the duplicated setting, and then set this again.
Maximum number of entries are already defined.	The number of VLAN settings specified by using `ip dhcp snooping vlan` exceeds the maximum number of specifiable items.
	The setting is not possible because the total number of configuration settings and dynamic learning items for `ip source binding` exceeds the maximum number of binding database entries. Delete unnecessary configuration settings or dynamic learning items, and then set this again.
	The number of VLANs set by using `ip arp inspection vlan` exceeds the maximum number of specifiable VLANs.
Relations between ip dhcp snooping configuration and channel-group configuration are inconsistent.	The applicable port cannot be set because it belongs to a channel group. Sets up a port channel interface.
Relations between ip dhcp snooping configuration and vlan mapping configuration are inconsistent.	vlan mapping cannot be specified for a trunk port in a VLAN for which the ip dhcp snooping vlan functionality is set.
Relations between ip dhcp snooping configuration and vlan-tunneling configuration are inconsistent.	The ip dhcp snooping vlan functionality and VLAN tunneling cannot be specified concurrently.

Message	Description
Relations between ip source binding configuration and channel-group configuration are inconsistent.	The specified port cannot be set because it belongs to a channel group or the specified port channel does not exist.
Relations between ip source binding configuration and switchport configuration are inconsistent.	The specified interface cannot be set because it does not belong to the VLAN.
Relations between ip verify source configuration and channel-group configuration are inconsistent.	The applicable port cannot be set because it belongs to a channel group. Sets up a port channel interface.

42.1.25 Uplink redundancy information

Table 42-25 Uplink redundancy error messages

Message	Description
Can't set ethernet *<IF#>* because it is a channel-group port.	The interface configuration cannot be changed because the specified interface belongs to a channel group. *<IF#>*: Interface port number
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
Ethernet *<IF#>* is already an uplink redundant interface.	The uplink redundant functionality has already been set for the specified interface. *<IF#>*: Interface port number
Ethernet *<IF#>* Relations between uplink redundant and the Ring Protocol are inconsistent.	The Ring Protocol functionality has already been set for the specified interface. Either delete the Ring Protocol functionality or specify another interface. *<IF#>*: Interface port number
Port-channel *<Channel group#>* is already an uplink redundant interface.	The uplink redundant functionality has already been set for the specified interface. *<Channel group#>*: Port channel number
Port-channel *<Channel group#>* Relations between uplink redundant and the Ring Protocol are inconsistent.	The Ring Protocol functionality has already been set for the specified interface. Either delete the Ring Protocol functionality or specify another interface. *<Channel group#>*: Port channel 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.
Secondary interface is same as primary interface.	The primary interface and the secondary interface are configured on the same port.
this command is different from this one in channel-group port.	Participation in the port channel is not possible because the configuration is different.
Too many parameters (exclude-VLAN).	The number of input parameters exceeds the maximum number (200). Set a value equal to or smaller than the maximum number.

42.1.26 SML (Split Multi Link) information [OS-L2A]

Table 42-26 SML (Split Multi Link) error messages

Message	Description
Cannot set the command because of internal error. (code=x)	The command could not be set because an internal error has occurred.
Peer-link parameter to allow is as follows: 24T:"0/25", "0/26","0/27" ,"0/28","0/25-26","0/27-28" 48T:"0/49", "0/50","0/51" ,"0/52","0/49-50","0/51-52"	The specified port cannot be set as a peer link port. (Version 3.0 or earlier)
Cannot set peer-link by the combination of this interface.	The specified port cannot be set as a peer link port. (Ver. 3.1 or later)
License key is not installed.	The license key has not been set.

42.1.27 Storm control information

Table 42-27 Storm control error messages

Message	Description
Please lower the recovery threshold than the detection threshold.	A value that is greater than the storm detection threshold is specified for the recovery-from-storm threshold. For the recovery-from-storm threshold, set a value equal to or smaller than the storm detection threshold.

42.1.28 L2 loop detection information

Table 42-28 L2 loop detection error messages

Message	Description
L2LD : Can't setting port[*<IF#>*] because of channel-group port.	The `loop-detection` command configuration cannot be changed because the specified port number belongs to a channel group. *<IF#>*: Interface port number
this command is different from this one in channel-group port.	Participation in the channel group is not possible because the `loop-detection` setting is different.

42.1.29 CFM information

Table 42-29 CFM error messages

Message	Description
ethernet : Can not delete it because data is not corresponding.	Deletion is not possible because the specified configuration does not exist or duplicate data exists.
ethernet : Cannot change cfm domain direction.	The MEP direction that is set in a domain cannot be changed. Delete the applicable command, and then set this again.

Message	Description
ethernet : Can't delete this configuration referred by other configuration.	The configuration cannot be changed because it is referenced by another configuration. Delete the configuration referenced by another configuration, and then set this again.
ethernet : MA *<No.>* is already configured in cfm domain.	The specified MA identification number is already being used by another domain. *<No.>*: MA identification number
ethernet : MA name *<Name>* is already configured in cfm domain.	The specified MA name is already set in the same domain. *<Name>*: MA name
ethernet : Maximum number of entries are already defined. *<CFM_MA>*	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.
ethernet : Not found *<Level>*.	The specified domain level cannot be found. Make sure the domain level has been set. *<Level>*: Domain level
ethernet : Not found *<No.>*.	The specified MA identification number cannot be found. Make sure the MA identification number has been set. *<No.>*: MA identification number
ethernet : Not found VLAN ID *<VLAN ID>* in MA.	The VLAN ID specified as the primary VLAN is not in the VLAN ID list. Specify a VLAN ID that has already been set in the MA. *<VLAN ID>*: VLAN ID
ethernet : Too many parameters (CFM_VLAN).	The number of input parameters exceeds the maximum number (256). Set a value equal to or smaller than the maximum number.
ethernet : 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
interface : Can not delete it because data is not corresponding.	Deletion is not possible because the specified configuration does not exist or duplicate data exists.
interface : Cannot change cfm mep direction.	The MEP direction cannot be changed. Delete the applicable command, and then set this again.
interface : Cannot configure cfm enable to channel-group port.	CFM of an interface participating in a port channel cannot be enabled.
interface : Cannot configure cfm mep to channel-group port.	An MEP cannot be set for an interface that is participating in a port channel.
interface : Cannot configure cfm mip to channel-group port.	An MIP cannot be set for an interface that is participating in a port channel.
interface : 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

Message	Description
interface : 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
interface : Exceeded the number of the maximum port.	The number of ports exceeds the number for which MEP and MIP can be set.
interface : Maximum number of entries are already defined. *<CFM_MEP>*	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.
interface : Maximum number of entries are already defined. *<CFM_MIP>*	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.
interface : MEP ID *<MEPID>* is already configured in cfm mep.	The specified MEP ID has already been set for another MEP. *<MEPID>*: MEP ID
interface : Not found *<Level>*.	The specified domain level cannot be found. Make sure the domain level has been set. *<Level>*: Domain level
interface : Not found *<No.>*.	The specified MA identification number cannot be found. Make sure the MA identification number has been set. *<No.>*: MA identification number

42.1.30 SNMP information

Table 42-30 SNMP error messages

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
interface : Can not delete it because data is not corresponding.	An attempt has been made to delete a non-existent identification number. Check the identification number.
interface : Maximum number of entries are already defined. *<RMON_HISTRY_CTR>*	The maximum number that has been set has been exceeded. Delete unnecessary entries.
interface : This configuration has already been set.	When the `rmon collection history` command was being set, it was found that the identification number was already being used by another interface. Either specify another identification number, or delete the identification number being used by the other interface, and then set the command again.
Maximum number of entries are already defined.	The maximum number that has been set has been exceeded. Delete unnecessary entries.

Message	Description
rmon : Can not delete it because data is not corresponding.	An attempt has been made to delete a non-existent identification number. Check the identification number.
rmon : Can't delete this configuration referred by other configuration.	The specified event entry cannot be deleted because it is associated with an alarm entry.
rmon : Maximum number of entries are already defined. *<RMON_ALARM>*	The maximum number that has been set has been exceeded. Delete unnecessary entries.
rmon : Maximum number of entries are already defined. *<RMON_EVENT>*	The maximum number that has been set has been exceeded. Delete unnecessary entries.
rmon : Can not delete it because data is not corresponding.	An attempt has been made to delete a non-existent identification number. Check the identification number.
rmon : Not found *<event_no>*.	A non-existent event identification number has been specified for `rising-event-index` or `falling-event-index`. Check `rising-event-index` or `falling-event-index` again. Alternatively, set an event identification number after setting the applicable event identification number.
rmon : Not supported *<variable>*.	An object that is not supported or an instance number that is not in the specifiable range is set for `variable`. Check the object and the instance number again.
rmon : RMON alarm rising threshold is less than falling threshold.	The lower threshold is greater than the upper threshold. Set a value smaller than the upper threshold as the lower threshold.
snmp-server: Maximum number of entries are already defined. *<SNMP_TRAP>*	The number of registered SNMP trap destination information items exceeds the maximum number. Delete unnecessary trap destination information, and then add the new item.
snmp-server: Maximum number of entries are already defined. *<SNMP_VIEW>*	The number of registered SNMP community information items exceeds the maximum number. Delete the unnecessary community information, and then add the new item.

42.1.31 Log Data Output Information

Table 42-31 Log data output error messages

Message	Description
Can't execute.	The command could not be executed. Re-execute the command.
logging : Can not delete it because data is not corresponding.	Deletion is unavailable because no event type is set.
too much number of the host.	Setting is unavailable because the maximum number of entries of the output destination is exceeded.

42.1.32 sFlow statistics

Table 42-32 sFlow statistics error messages

Message	Description
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.
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 switch. 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.
This system doesn't support "sflow forward egress" the command.	The `sflow forward egress` command cannot be used because it is not supported by the Switch.

42.1.33 Port mirroring information

Table 42-33 Port mirroring error messages

Message	Description
Cannot set the command because the SML is enabled.	The command cannot be set because the SML functionality is enabled.
Mirror port and dot1x are inconsistent.	The destination interface cannot be set as a mirror port because the destination interface is being used by `dot1x`.
Mirror port and mac-authentication are inconsistent.	The destination interface cannot be set as a mirror port because the destination interface is being used for MAC-based authentication.
Mirror port and web-authentication are inconsistent.	The destination interface cannot be set as a mirror port because the destination interface is being used for Web authentication.
Mirror port and mac-address-table are inconsistent.	The destination interface cannot be set as a mirror port because the destination interface is being used for `mac-address-table`.
Mirror port and port-channel are inconsistent.	The destination interface cannot be set as a mirror port because it is being used by the port channel.
Mirror port and switchport are inconsistent.	Both mirror port and switchport settings cannot be specified simultaneously.

Index