AX2340S Software Manual

Configuration Command Reference

For Version 2.5

AX23S-S003X-60

AlaxalA

■ Relevant products

This manual applies to the models in the AX2340S series of switches. It also describes the function of OS-L2N version 2.5 of the software.

■ Precautions in exporting

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

■ Trademarks

■ Reading and storing this manual

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

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

■ Note

Information in this document is subject to change without notice.

■ Editions history

June 2024 (Edition 1) AX23S-S003X-60

■ Copyright

Preface

■ Applicable products and software versions

This manual applies to the models in the AX2340S series of switches. It also describes the functions supported by the software OS-L2N Ver. 2.5 and optional licenses.

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

■ Corrections to the manual

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

■ Intended readers

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

Readers must have an understanding of the following:

- The basics of network system management

■ Manual URL

You can view this manual on our website at:

https://www.alaxala.com/en/

■ Reading sequence of the manuals

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

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

Hardware Instruction Manual (AX23S-H001X)

Transceiver Hardware Instruction Manual (AX-COM-H001X)

● To learn the software functions, commands, and configuration settings

Configuration Guide Vol.1 (AX23S-S001X)

Vol.2 (AX23S-S002X)

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

Configuration Command Reference (AX23S-S003X)

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

Operation Command Reference (AX23S-S004X)

● To check messages and logs

Message Log Reference (AX23S-S005X)

● To learn how to troubleshoot a problem

Troubleshooting Guide (AX23S-T001X)

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

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

- AX2340S series switch

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

■ Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
bit/s	bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
CA	Certificate Authority

CBC	Cipher Block Chaining
CC	Continuity Check
CFM	Connectivity Fault Management
CIST	Common and Internal Spanning Tree
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRR	Deficit Round Robin
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEE	Energy Efficient Ethernet
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance

OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PoE	Power over Ethernet
PQ	Priority Queueing
PS	Power Supply
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RMON	Remote Network Monitoring MIB
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual LAN
WAN	Wide Area Network
WWW	World-Wide Web

■ Conventions: KB, MB, GB, and TB

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

Contents

PART 1: Reading the Manual

1. Reading the Manual 21

Command description format 22
Command mode list 23
Specifiable values for parameters 25

PART 2: Operation Management

2. Operation Terminal Connection 31

ftp-server 32
line console 33
line vty 34
speed 35
transport input 36

3. Configuration Editing and Operation 39

end 40
quit (exit) 42
save (write) 44
show 46
status 47
top 49

4. Login Security and RADIUS/TACACS+ 51

aaa accounting commands 52
aaa accounting exec 54
aaa authentication enable 56
aaa authentication enable attribute-user-per-method 57
aaa authentication enable end-by-reject 58
aaa authentication login 59
aaa authentication login console 60
aaa authentication login end-by-reject 61
aaa authorization commands 62
aaa authorization commands console 64
banner 65
commands exec 69
ip access-group 71
ipv6 access-class 73
parser view 74
radius-server host 75

radius-server key 78
radius-server retransmit 79
radius-server timeout 80
tacacs-server host 81
tacacs-server key 83
tacacs-server timeout 84
username 85

5. SSH 89

ip ssh 90
ip ssh authentication 91
ip ssh authkey 92
ip ssh ciphers 94
ip ssh key-exchange 95
ip ssh macs 96
ip ssh version 97

6. Time Settings and NTP 99

clock timezone 100
ntp access-group 102
ntp authenticate 104
ntp authentication-key 105
ntp broadcast 106
ntp broadcast client 108
ntp broadcastdelay 109
ntp master 110
ntp peer 111
ntp server 113
ntp trusted-key 115

7. Host Names and DNS 117

ip domain lookup 118
ip domain name 119
ip domain reverse-lookup 120
ip host 121
ip name-server 122
ipv6 host 124

8. Device Management 125

switch provision 126
system fan mode 128
system l2-table mode 129
system memory-soft-error 130
system recovery 131

system temperature-warning-level 132

9. Zero-touch Provisioning 133

system zero-touch-provisioning 134
system zero-touch-provisioning vlan 135

10. Power Saving Functions 137

eee enable 138

11. Log Data Output Function 139

logging email 140
logging email-event-kind 142
logging email-from 143
logging email-interval 144
logging email-server 145
logging event-kind 147
logging facility 148
logging host 149
logging syslog-dump 151
logging syslog-version 152
logging trap 153

12. SNMP 155

hostname 156
rmon alarm 157
rmon collection history 160
rmon event 162
snmp-server community 164
snmp-server contact 166
snmp-server engineID local 167
snmp-server group 169
snmp-server host 172
snmp-server informs 177
snmp-server location 179
snmp-server traps 180
snmp-server user 183
snmp-server view 185
snmp trap link-status 187

13. Advanced Script 189

aaa authorization commands script 190
action 192
disable 194
event manager applet 195
event sysmsg 196

event timer 199
priority 202
resident-script 204

PART 3: Network Interfaces

14. Ethernet 207

bandwidth 208
description 209
duplex (gigabitethernet) 210
duplex (tengigabitethernet) 212
flowcontrol 214
frame-error-notice 217
interface gigabitethernet 220
interface tengigabitethernet 221
link debounce 222
link up-debounce 223
mdix auto 224
mtu 225
power inline 227
power inline allocation 229
power inline delay 231
power inline priority-control disable 233
shutdown 234
speed (gigabitethernet) 235
speed (tengigabitethernet) 238
system flowcontrol off 240
system mtu 241

15. Link Aggregation 243

channel-group lacp system-priority 244
channel-group max-active-port 245
channel-group max-detach-port 247
channel-group mode 249
channel-group periodic-timer 251
description 252
interface port-channel 253
lacp port-priority 254
lacp system-priority 255
shutdown 256

PART 4: Layer 2 Switching

16. MAC Address Table 257

mac-address-table aging-time 258
mac-address-table learning 259
mac-address-table static 261

17. VLAN 263

down-debounce 264
interface vlan 265
l2protocol-tunnel eap 266
l2protocol-tunnel stp 267
mac-address 268
name 269
protocol 270
state 271
switchport access 272
switchport dot1q ethertype 273
switchport isolation 274
switchport mac 276
switchport mode 279
switchport protocol 281
switchport trunk 283
switchport validation 285
switchport vlan mapping 287
switchport vlan mapping enable 289
up-debounce 290
vlan 291
vlan-dot1q-ethertype 294
vlan-protocol 295
vlan-up-message 297

18. Spanning Tree Protocols 299

instance 300
name 302
revision 303
spanning-tree bpdufilter 304
spanning-tree bpduguard 305
spanning-tree cost 306
spanning-tree disable 308
spanning-tree guard 309
spanning-tree link-type 311
spanning-tree loopguard default 312
spanning-tree mode 313
spanning-tree mst configuration 314
spanning-tree mst cost 315
spanning-tree mst forward-time 317

spanning-tree mst hello-time 318
spanning-tree mst max-age 319
spanning-tree mst max-hops 320
spanning-tree mst port-priority 321
spanning-tree mst root priority 323
spanning-tree mst transmission-limit 324
spanning-tree pathcost method 325
spanning-tree port-priority 327
spanning-tree portfast 328
spanning-tree portfast bpduguard default 329
spanning-tree portfast default 330
spanning-tree single 331
spanning-tree single cost 332
spanning-tree single forward-time 333
spanning-tree single hello-time 334
spanning-tree single max-age 335
spanning-tree single mode 336
spanning-tree single pathcost method 337
spanning-tree single port-priority 339
spanning-tree single priority 340
spanning-tree single transmission-limit 341
spanning-tree vlan 342
spanning-tree vlan cost 343
spanning-tree vlan forward-time 345
spanning-tree vlan hello-time 347
spanning-tree vlan max-age 348
spanning-tree vlan mode 349
spanning-tree vlan pathcost method 350
spanning-tree vlan port-priority 352
spanning-tree vlan priority 354
spanning-tree vlan transmission-limit 355

19. Ring Protocol 357

axrp 358
axrp vlan-mapping 359
axrp-ring-port 361
control-vlan 363
disable 365
forwarding-shift-time 366
mac-clear-mode 367
mode 368
multi-fault-detection mode 369
multi-fault-detection vlan 370

name 371
vlan-group 372

20. IGMP snooping 375
ip igmp snooping (global) 376
ip igmp snooping (VLAN interface) 377
ip igmp snooping fast-leave 378
ip igmp snooping mrouter 379
ip igmp snooping mrouter discovery 380
ip igmp snooping mrouter discovery extension 382
ip igmp snooping mrouter logging 383
ip igmp snooping querier 384
ip igmp snooping query-interval 385

21. MLD snooping 387
ipv6 mld snooping (global) 388
ipv6 mld snooping (VLAN interface) 389
ipv6 mld snooping mrouter 390
ipv6 mld snooping querier 391

PART 5: IP Interface

22. IPv4 Communication 393
arp 394
arp max-send-count 396
arp send-interval 397
arp timeout 398
ip address 399
ip mtu 401
ip route 402

23. IPv6 Communication 405
ipv6 address 406
ipv6 enable 408
ipv6 icmp error-interval 409
ipv6 nd accept-ra 410
ipv6 neighbor 412
ipv6 route 414

24. Loopback Interface 417
interface loopback 418
ip address (loopback) 419
ipv6 address (loopback) 420

25. DHCP Server Function 421

client-name 422
default-router 423
dns-server 424
domain-name 425
hardware-address 426
host 427
ip dhcp dynamic-dns-update 429
ip dhcp excluded-address 430
ip dhcp key 431
ip dhcp pool 432
ip dhcp zone 433
lease 435
max-lease 437
netbios-name-server 439
netbios-node-type 440
network 441
service dhcp 443

PART 6: Filters and QoS

26. Flow Detection Modes/Flow Performance 445
flow detection mode 446

27. Access Lists 449
Names and values that can be specified 450
access-list 461
deny (ip access-list extended) 469
deny (ip access-list standard) 475
deny (ipv6 access-list) 477
deny (mac access-list extended) 483
ip access-group 486
ip access-list extended 488
ip access-list resequence 490
ip access-list standard 492
ipv6 access-list 494
ipv6 access-list resequence 495
ipv6 traffic-filter 497
mac access-group 499
mac access-list extended 501
mac access-list resequence 502
permit (ip access-list extended) 504
permit (ip access-list standard) 510
permit (ipv6 access-list) 512
permit (mac access-list extended) 518

remark 521

28. QoS 523

Names and values that can be specified 524
ip qos-flow-group 535
ip qos-flow-list 537
ip qos-flow-list resequence 538
ipv6 qos-flow-group 540
ipv6 qos-flow-list 542
ipv6 qos-flow-list resequence 543
mac qos-flow-group 545
mac qos-flow-list 547
mac qos-flow-list resequence 548
qos (ip qos-flow-list) 550
qos (ipv6 qos-flow-list) 557
qos (mac qos-flow-list) 564
qos-queue-group 568
qos-queue-list 569
remark 571
traffic-shape rate 572

PART 7: Layer 2 Authentication

29. Layer 2 Authentication 575

Configuration command and applicable Layer 2 authentication types 576
authentication arp-relay 577
authentication auto-logout strayer 578
authentication force-authorized enable 579
authentication force-authorized vlan 580
authentication ip access-group 581
authentication logout linkdown 582
authentication mac access-group 583
authentication max-user (global) 584
authentication max-user (interface) 585
authentication radius-server dead-interval 586

30. IEEE 802.1X 587

aaa accounting dot1x default 588
aaa authentication dot1x default 589
dot1x auto-logout 590
dot1x ignore-eapol-start 591
dot1x logging enable 592
dot1x loglevel 593
dot1x max-req 595

dot1x max-supplicant 596
dot1x multiple-authentication 597
dot1x multiple-hosts 598
dot1x port-control 599
dot1x radius-server host 601
dot1x reauthentication 603
dot1x supplicant-detection 604
dot1x system-auth-control 606
dot1x timeout keep-unauth 607
dot1x timeout quiet-period 608
dot1x timeout reauth-period 609
dot1x timeout server-timeout 610
dot1x timeout supp-timeout 611
dot1x timeout tx-period 612

31. Web Authentication 613

Correspondence between configuration commands and running modes 614
aaa accounting web-authentication default start-stop group radius 616
aaa authentication web-authentication default group radius 617
web-authentication auto-logout 618
web-authentication connection-pool level 619
web-authentication html-fileset 620
web-authentication ip address 621
web-authentication jump-url 623
web-authentication logging enable 624
web-authentication logout ping tos-windows 625
web-authentication logout ping ttl 626
web-authentication logout polling count 627
web-authentication logout polling enable 629
web-authentication logout polling interval 631
web-authentication logout polling retry-interval 633
web-authentication max-timer 635
web-authentication max-user 636
web-authentication port 637
web-authentication radius-server host 638
web-authentication redirect enable 640
web-authentication redirect-mode 641
web-authentication ssl connection-timeout 642
web-authentication static-vlan max-user 643
web-authentication system-auth-control 644
web-authentication user replacement 645
web-authentication web-port 646

32. MAC-based Authentication 649

Correspondence between configuration commands and running modes 650
aaa accounting mac-authentication default start-stop group radius 652
aaa authentication mac-authentication default group radius 653
mac-authentication auth-interval-timer 654
mac-authentication auto-logout 655
mac-authentication dot1q-vlan force-authorized 656
mac-authentication dynamic-vlan max-user 657
mac-authentication id-format 658
mac-authentication logging enable 660
mac-authentication login-failed-logging disable 661
mac-authentication max-timer 662
mac-authentication password 663
mac-authentication port 664
mac-authentication radius-server host 665
mac-authentication static-vlan max-user 667
mac-authentication system-auth-control 668
mac-authentication timeout reauth-period 669
mac-authentication vlan-check 670

33. Multistep Authentication 671

authentication multi-step 672

PART 8: Security

34. DHCP snooping 673

ip arp inspection limit rate 674
ip arp inspection trust 675
ip arp inspection validate 676
ip arp inspection vlan 678
ip dhcp snooping 680
ip dhcp snooping database url 681
ip dhcp snooping database write-delay 683
ip dhcp snooping information option allow-untrusted 684
ip dhcp snooping limit rate 685
ip dhcp snooping logging enable 686
ip dhcp snooping loglevel 687
ip dhcp snooping trust 689
ip dhcp snooping verify mac-address 690
ip dhcp snooping vlan 691
ip source binding 693
ip verify source 695

PART 9: High Reliability Based on Redundant Configurations

35. Uplink Redundancy 697

switchport backup flush-request transmit 698
switchport backup interface 699
switchport backup mac-address-table update exclude-vlan 701
switchport backup mac-address-table update transmit 703
switchport backup reset-flush-port 704
switchport backup reset-flush-time 705
switchport-backup startup-active-port-selection 706

PART 10: Network Monitoring Function

36. L2 Loop Detection 707

loop-detection 708
loop-detection auto-restore-time 710
loop-detection enable 711
loop-detection hold-time 712
loop-detection interval-time 713
loop-detection threshold 714

37. Storm Control 715

storm-control 716

PART 11: Network Management

38. Port Mirroring 721

monitor session 722

39. sFlow Statistics 725

sflow destination 726
sflow extended-information-type 727
sflow forward egress 729
sflow forward ingress 730
sflow max-header-size 731
sflow max-packet-size 732
sflow packet-information-type 733
sflow polling-interval 734
sflow sample 735
sflow source 738
sflow url-port-add 740
sflow version 741

40. IEEE 802.3ah/UDLD 743

efmoam active 744

efmoam disable 745
efmoam udld-detection-count 746

41. CFM 747

domain name 748
ethernet cfm cc alarm-priority 750
ethernet cfm cc alarm-reset-time 752
ethernet cfm cc alarm-start-time 754
ethernet cfm cc enable 756
ethernet cfm cc interval 757
ethernet cfm domain 759
ethernet cfm enable (global) 761
ethernet cfm enable (interface) 762
ethernet cfm mep 763
ethernet cfm mip 765
ma name 766
ma vlan-group 768

42. LLDP 771

lldp enable 772
lldp hold-count 773
lldp interval-time 774
lldp management-address 775
lldp run 776

PART 12: Configuration Error Messages

43. Error Messages Displayed When Editing the Configuration 777

43.1 Error messages displayed when editing the configuration 778
43.1.1 Common 778
43.1.2 Configuration editing and operation information 779
43.1.3 Login security and RADIUS/TACACS+ information 781
43.1.4 SSH information 781
43.1.5 Host names and DNS information 782
43.1.6 Device management information 782
43.1.7 Zero-touch provisioning information 782
43.1.8 SNMP information 782
43.1.9 Advanced script information 783
43.1.10 Ethernet information 783
43.1.11 Link aggregation information 784
43.1.12 MAC address table information 785
43.1.13 VLAN information 785

43.1.14 Spanning Tree information 788
43.1.15 Ring Protocol information 788
43.1.16 IGMP snooping information 790
43.1.17 MLD snooping information 790
43.1.18 IPv4 communication information 791
43.1.19 IPv6 communication information 792
43.1.20 DHCP server function 793
43.1.21 Flow detection modes/flow performance information 794
43.1.22 Access list information 794
43.1.23 QoS information 795
43.1.24 Layer 2 authentication information 796
43.1.25 IEEE 802.1X information 797
43.1.26 Web authentication information 799
43.1.27 MAC-based authentication information 800
43.1.28 DHCP snooping information 800
43.1.29 Uplink redundancy information 800
43.1.30 Storm control information 801
43.1.31 Port mirroring information 801
43.1.32 sFlow statistics information 802
43.1.33 CFM information 802

1 Reading the Manual

Command description format

Each command is described in the following format:

Function

Describes the purpose of the command.

Syntax

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

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

Input mode

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

Parameters

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

Default behavior

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

Impact on communication

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

When the change is applied

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

Notes

Provides cautionary information on using the command.

Command mode list

The following table lists the command modes.

Table 1-1: List of configuration commands

No.	Prompt displayed for the command mode	Description of command mode	Mode transition command
1	(config)	Global configuration mode	# enable # configure
2	(config-line)	Configuring remote login and console settings	(config)# line vty (config)# line console
3	(config-if)	Configuring an Ethernet interface	(config)# interface gigabitethernet (config)# interface tengigabitethernet
		Configuring a port channel interface	(config)# interface port-channel
		Configuring a VLAN interface	(config)# interface vlan
		Configuring a loopback interface	(config)# interface loopback
4	(config-if-range)	Configuring multiple Ethernet interfaces	(config)# interface range gigabitethernet (config)# interface range tengigabitethernet
		Configuring multiple port channel interfaces	(config)# interface range port-channel
		Configuring multiple VLAN interfaces	(config)# interface range vlan
5	(config-vlan)	Configuring a VLAN	(config)# vlan
6	(config-mst)	Configuring Multiple Spanning Tree	(config)# spanning-tree mst configuration
7	(config-axrp)	Configuring the Ring Protocol	(config)# axrp
8	(config-ext-nacl)	Configuring an IPv4 packet filter	(config)# ip access-list extended
9	(config-std-nacl)	Configuring an IPv4 address filter	(config)# ip access-list standard
10	(config-ipv6-acl)	Configuring an IPv6 filter	(config)# ipv6 access-list
11	(config-ext-macl)	Configuring a MAC filter	(config)# mac access-list extended
12	(config-ip-qos)	Configuring IPv4 QoS	(config)# ip qos-flow-list
13	(config-ipv6-qos)	Configuring IPv6 QoS	(config)# ipv6 qos-flow-list
14	(config-mac-qos)	Configuring MAC QoS	(config)# mac qos-flow-list
15	(dhcp-config)	Configuring DHCP	(config)# ip dhcp pool
16	(config-view)	Configuring view	(config)# parser view
17	(config-ether-cfm)	Configuring the domain name and MA	(config)# ethernet cfm domain

No.	Prompt displayed for the command mode	Description of command mode	Mode transition command
18	(config-applet)	Configuring the applet functions	(config)# event manager applet <applet name>

Specifiable values for parameters

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

Table 1-2: Specifiable values for parameters

Parameter type	Description	Input example
Name	Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), underscores (_), and periods (.) can be used for the second and subsequent characters.	ip access-list standard inbound1
Host name	For a host name, alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and periods (.) can be used for the second and subsequent characters.	ip host telnet-host 192.168.1.1
IPv4 address, Subnet mask	Specify these 4-byte items in decimal format, separating 1-byte decimal values by a period (.).	192.168.0.14 255.255.255.0
Wildcard mask	The same input format as IPv4 addresses. The set bits in an IPv4 address represent an arbitrary value.	255.255.0.0
IPv6 address	Specify this item in hexadecimal format, separating 2-byte hexadecimal values by colons (:).	3ffe:501:811:ff03::87ff:fed0:c7e0
add/remove specification	Add to or delete from the information when multiple items have been specified. The add specification adds information to the current information. The remove specification deletes information from the current information.	switchport trunk allowed vlan add 100,200-210 switchport trunk allowed vlan remove 100,200-210 switchport isolation interface add gigabitethernet 1/0/1-3, tengigabitethernet 1/0/27-28 switchport isolation interface remove gigabitethernet 1/0/1-3, tengigabitethernet 1/0/27-28

■ Arbitrary character string

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

Table 1-3: List of character codes

Character	Code	Character	Code	Character	Code	Character	Code	Character	Code	Character	Code
Space	0x20	0	0x30	@	0x40	P	0x50	`	0x60	p	0x70
!	0x21	1	0x31	A	0x41	Q	0x51	a	0x61	q	0x71
"	0x22	2	0x32	B	0x42	R	0x52	b	0x62	r	0x72
#	0x23	3	0x33	C	0x43	S	0x53	c	0x63	s	0x73
$	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

Char-acter	Code	Char-acter	Code	Char-acter	Code	Char-acter	Code	Char-acter	Code	Char-acter	Code
'	0x27	7	0x37	G	0x47	W	0x57	g	0x67	w	0x77
(	0x28	8	0x38	H	0x48	X	0x58	h	0x68	x	0x78
)	0x29	9	0x39	I	0x49	Y	0x59	i	0x69	y	0x79
*	0x2A	:	0x3A	J	0x4A	Z	0x5A	j	0x6A	z	0x7A
+	0x2B	;	0x3B	K	0x4B	[	0x5B	k	0x6B	{	0x7B
,	0x2C	<	0x3C	L	0x4C	\	0x5C	l	0x6C	|	0x7C
-	0x2D	=	0x3D	M	0x4D	]	0x5D	m	0x6D	}	0x7D
.	0x2E	>	0x3E	N	0x4E	^	0x5E	n	0x6E	~	0x7E
/	0x2F	?	0x3F	O	0x4F	_	0x5F	o	0x6F	---	---

Notes

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

Special characters that cannot be specified

Table 1-4: Special characters that cannot be specified

Character name	Character	Code
Double quotation mark	"	0x22
Dollar sign	$	0x24
Single quotation mark	'	0x27
Semicolon	;	0x3B
Backslash	\	0x5C
Grave accent mark	`	0x60
Left curly bracket	{	0x7B
Right curly bracket	}	0x7D

Example of specification string

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

■ Range of <switch no.>, <nif no.>, and <port no.> values

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

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

Model	Range of values		
	<switch no.>	<nif no.>	<port no.>
AX2340S-16T4X	1	0	1 to 20
AX2340S-24T4X			1 to 30
AX2340S-24TH4X			1 to 30
AX2340S-48T4X			1 to 54
AX2340S-24P4X			1 to 30
AX2340S-24PH4X			1 to 30
AX2340S-48P4X			1 to 54
AX2340S-16P8MP2X			1 to 26

Table 1-6: Range of <switch no.>, <nif no.> and <port no.> values (when specifying PoE port)

Model	Range of values		
	<switch no.>	<nif no.>	<port no.>
AX2340S-24P4X	1	0	1 to 24
AX2340S-24PH4X			1 to 24
AX2340S-48P4X			1 to 48
AX2340S-16P8MP2X			1 to 24

■ How to specify <interface id list>

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

- For Gigabit Ethernet interfaces

  gigabitethernet <switch no.>/<nif no.>/<port no.>[-<port no.>]
- For 10 Gigabit Ethernet interfaces

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

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

gigabitethernet 1/0/1-2, gigabitethernet 1/0/5, tengigabitethernet 1/0/27-28

■ Range of <channel group number> values

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

Table 1-7: Range of <channel group number> values

No.	Model	Range of values
1	All models	1 to 120

■ Range of <vlan id> values

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

■ How to specify <vlan id list>

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

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

1-3,5,10

Example of a specification displayed in multiple lines

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

switchport trunk allowed vlan add 400,500...

■ How to specify the interface

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

Table 1-8: How to specify an interface

Interface type group	Interface type to be specified in <interface type>	Interface number to be specified in <interface number>
Ethernet interface	gigabitethernet	<switch no.>/<nif no.>/<port no.>
	tengigabitethernet	<switch no.>/<nif no.>/<port no.>
Port channel interface	port-channel	<channel group number>
VLAN interface	vlan	<vlan id>
Loopback interface	loopback	0

■ Specification of multiple interfaces

This specification method is used to collectively set the same information for multiple interfaces. You can specify the interface names and interface numbers that correspond to the following interface type groups among the groups listed in "Table 1-8: How to specify an interface".

- Ethernet interface
- Port channel interface
- VLAN interface

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

Syntax

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

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

Input example

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

■ Specifiable values for the message type

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

Table 1-9: Specifiable values for the message type

No.	Specifiable value
1	key
2	rsp
3	sky
4	srs
5	err
6	evt
7	aut
8	dsn

2 Operation Terminal Connection

ftp-server

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

Syntax

To set information:

ftp-server

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

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

line console

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

Syntax

To set information:

line console 0

To delete information:

no line console

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

line vty

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

Syntax

To set information:

line vty 0 <number>

To delete information:

no line vty

Input mode

```
(config)
```

Parameters

<number>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

Does not accept remote login that uses Telnet or SSH.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. 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.

speed

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

Syntax

To set or change information:

speed <number>

To delete information:

no speed

Input mode

```
(config-line)
```

Parameters

<number>

Sets the communication speed for CONSOLE (RS232C) in bit/s.

1. Default value when this parameter is omitted:

   Sets the communication speed of CONSOLE (RS232C) to 115200bit/s.

2. Range of values:

   2400, 4800, 9600, 19200

Default behavior

The communication speed of CONSOLE (RS232C) is 115200bit/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.

transport input

Restricts access from remote operation terminals based on protocol.

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

Syntax

To set or change information:

transport input {telnet | ssh | all | none}

To delete information:

no transport input

Input mode

```
(config-line)
```

Parameters

{telnet | ssh | all | none}

telnet

Accepts remote access that uses the Telnet protocol.

ssh

Accepts remote access that uses the SSH protocol.

all

Accepts remote access that uses any protocol.

none

Does not accept remote access using any protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

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

3 Configuration Editing and Operation

end

Ends configuration command mode and returns you to administrator mode.

Syntax

end

Input mode

Configuration command mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

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

Table 3-1: Response messages for the end command

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

Notes

1. You can use this command to temporarily exit configuration command mode without saving the configuration in the startup configuration file. If you do so, the editing process of the configuration will still be incomplete. Once editing the configuration is completed, execute the "save" command to save it in the startup configuration file.
2. If you execute this command without saving the edited configuration in the startup configuration file, the configuration will differ from the startup configuration file. For this reason, if you enter configuration command mode again and then enter this command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.
3. Do not press the Ctrl + C keys to interrupt processing while this command is being executed. If the pro-

cessing is interrupted, configuration command mode will not end. Then, executing a configuration command might cause an error with the message: Logical inconsistency occurred. If this message is output, use this command to end configuration command mode.

quit (exit)

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

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

Syntax

quit or exit

Input mode

Configuration command mode, user mode, and administrator mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

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

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

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

Notes

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

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

the startup configuration file.

2. If you execute this command without saving the edited configuration in the startup configuration file, the configuration will differ from the startup configuration file. For this reason, if you enter configuration command mode again and then enter this command, the same confirmation message will be displayed even if you have not made any new changes to the configuration file.
3. Do not press the Ctrl + C keys to interrupt processing while this command is being executed. If the processing is interrupted, configuration command mode will not end. Then, executing a configuration command might cause an error with the message: Logical inconsistency occurred. If this message is output, use the "end" command to end configuration command mode.

save (write)

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

Syntax

save [<file name>] [debug]

write [<file name>] [debug]

Input mode

Configuration command mode

Parameters

<file name>

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

- Specifying a local configuration file

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

- Specifying a remotely-stored configuration file

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

  - FTP

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

  - TFTP

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

1. Default value when this parameter is omitted:

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

debug

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

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

Default behavior

None

Impact on communication

None

When the change is applied

None

Response messages

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

Table 3-3: Response messages for the save command

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

Notes

1. Saving the configuration file does not exit configuration command mode. To finish editing and exit configuration command mode, use the "exit" command or "end" command.
2. If you do not have permission to write the configuration file to the save destination, your edits are not saved to the file. To save edits to a file on a remote server, your remote server access permissions must be changed to allow you to write to the remote server.
3. You can use the "status" command to check if the configuration has been changed but not saved.
4. If there is insufficient free capacity in internal flash memory, changed configurations cannot be saved. Use the "show flash" operation command to check the free capacity in the user area. Saving a new startup configuration file (/config/system.cnf) requires free capacity equivalent to the size of the existing startup configuration file (/config/system.cnf) plus the size of the configuration you are editing. About 2 MB of free capacity is required for a maximum-size configuration file.
5. If you execute this command when the memory card operation mode is enabled, the "update mc-configuration" operation command will also be executed automatically. Therefore, the operation log corresponding to the "update mc-configuration" operation command is collected. For details about the operation log, see the "Message Log Reference". Note that even if an error is detected during the processing of the "update mc-configuration" operation command, this command ends normally.

show

Displays the configuration being edited.

Syntax

show [<command> [<parameter>]]

Input mode

Configuration command mode

Parameters

<command>

Specifies a configuration command.

<parameter>

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

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If there are many items in the configuration, the command might take time to execute.
2. If the configuration is edited or the "copy" command is executed while this command is being executed, this command might be aborted.
3. When software is updated, the last-modified time displayed on the first line before and after the device is restarted might be slightly inaccurate.

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

status

Shows the status of the configuration being edited.

Syntax

status

Input mode

Configuration command mode

Parameters

None

Displayed information

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

Table 3-4: Response messages for the status command

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

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. If the remaining capacity becomes very small, it might not be sufficient to execute some configuration commands.
2. Before and after a device is restarted, the last-modified time displayed on the first line might be slightly inaccurate.

top

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

Syntax

top

Input mode

Configuration command mode

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

None

4 Login Security and RADIUS/ TACACS+

aaa accounting commands

Logs accounting information when commands are used.

Syntax

To set or change information:

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

To delete information:

no aaa accounting commands

Input mode

```
(config)
```

Parameters

{ 15 | 0-15 }

Specifies the command level for accounting.

15

Only configuration commands are subject to accounting.

0-15

Both operation commands and configuration commands are subject to accounting.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

{start-stop | stop-only}

Specifies the trigger of accounting for commands.

start-stop

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

stop-only

Sends a stop instruction before a command is executed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

broadcast

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

1. Default value when this parameter is omitted:

   Accounting information will be repeatedly sent in turn to a maximum of four servers until it is suc-

cessfully sent to, and acknowledgements are received from, the servers.

group tacacs+

The TACACS+ server is used as the accounting server.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

aaa accounting exec

Enables accounting of login and logout.

Syntax

To set or change information:

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

To delete information:

no aaa accounting exec

Input mode

```
(config)
```

Parameters

{start-stop | stop-only}

Sets the trigger for accounting.

start-stop

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

stop-only

Sends a stop instruction at logout only.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

broadcast

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

1. Default value when this parameter is omitted:

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

{group radius | group tacacs+}

Sets the type of an accounting server.

group radius

The RADIUS server is used as the accounting server.

group tacacs+

The TACACS+ server is used as the accounting server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

aaa authentication enable

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

Syntax

To set or change information:

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

To delete information:

no aaa authentication enable

Input mode

```
(config)
```

Parameters

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

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

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

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

enable

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

aaa authentication enable attribute-user-per-method

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

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

Syntax

To set information:

aaa authentication enable attribute-user-per-method

To delete information:

no aaa authentication enable attribute-user-per-method

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

aaa authentication enable end-by-reject

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

Syntax

To set information:

aaa authentication enable end-by-reject

To delete information:

no aaa authentication enable end-by-reject

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

aaa authentication login

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

Syntax

To set or change information:

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

To delete information:

no aaa authentication login

Input mode

```
(config)
```

Parameters

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

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

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

group radius

RADIUS authentication is used.

group tacacs+

TACACS+ authentication is used.

local

Local password authentication is used.

Default behavior

Local password authentication is performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

aaa authentication login console

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

Syntax

To set information:

aaa authentication login console

To delete information:

no aaa authentication login console

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To perform RADIUS/TACACS+ authentication, you must set the "aaa authentication login" command at the same time.
2. When the <local> parameter is not specified as the authentication method by the "aaa authentication login" command, and the "aaa authentication login console" command is set, the user cannot log in from the console (RS232C) if communication with a RADIUS/TACACS+ server is impossible or authentication fails.

aaa authentication login end-by-reject

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

Syntax

To set information:

aaa authentication login end-by-reject

To delete information:

no aaa authentication login end-by-reject

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

aaa authorization commands

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

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

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

Syntax

To set or change information:

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

To delete information:

no aaa authorization commands

Input mode

```
(config)
```

Parameters

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

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

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

group radius

Command authorization is performed by a RADIUS server.

group tacacs+

Command authorization is performed by a TACACS+ server.

local

Local command authorization is performed.

Default behavior

Command authorization is not performed.

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. With this setting, the command class or command list is obtained simultaneously when command authorization is performed on the RADIUS server or TACACS+ server or by using a local password, as specified by the "aaa authentication login" command. The "aaa authorization commands" command alone is not sufficient for command authorization. You also need to have used the "aaa authentication login" command in advance.
2. After successful login, you will not be authorized to execute any commands except "logout", "exit", "quit", "disable", "end", "set terminal", "show whoami", and "who am i" if any of the following applies:
   - If the command class or the command list cannot be obtained as a vendor-specific attribute or an attribute value when authentication is performed on a RADIUS server or a TACACS+ server
   - If the user name and the associated command class (username view-class) or command list (username view) are not configured when authentication is performed using a local password

aaa authorization commands console

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

Syntax

To set information:

aaa authorization commands console

To delete information:

no aaa authorization commands console

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. The "aaa authorization commands console" command alone is not sufficient for command authorization. You also need to set the "aaa authorization commands" command.
2. With this setting, if a user logs in from the console (RS232C), command authorization is used to restrict the commands that can be executed.

banner

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

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

Table 4-1: List of pre-login messages to be displayed according to settings

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

Table 4-2: List of post-login messages to be displayed according to settings

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

Syntax

To set or change information:

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

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

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

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

To delete information:

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

Input mode

```
(config)
```

Parameters

login

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

plain-text

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

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

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

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

1. Default value when this parameter is omitted:
   No login messages are displayed.
2. Range of values:
   A string consisting of a maximum of 720 alphanumeric characters
3. Note on using this parameter:
   When entering login messages, check the screen settings for the client so that you do not use characters that cannot be displayed on the client. Otherwise, when the "show banner {motd | motd-ftp | login | login-ftp } plain-text" command is executed or a client is connected, the prompt might be garbled and the screen display might freeze. If you want to cancel login message setting while entering the login message, press the Ctrl+C keys to abort this. If you enter far more characters than the maximum number of characters permitted in a line, you may find that no further keyboard input (including the Ctrl+D keys or a line break) is accepted. If this happens, use the Backspace key to delete entered characters and then re-enter them, or use the Ctrl+C keys to abort.

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

encode "<encoded message>"

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

1. Default value when this parameter is omitted:
   No login messages are displayed.
2. Range of values:
   Enter a Base64-encoded string enclosed in double-quotation marks (") (a maximum of 960 characters).

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

login-ftp

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

plain-text

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

encode "<encoded message>"

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

disable

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

motd

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

plain-text

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

encode "<encoded message>"

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

motd-ftp

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

plain-text

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

encode "<encoded message>"

Enter a Base64-encoded string as a login message.

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

disable

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

Default behavior

No login messages are displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

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

commands exec

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

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

Syntax

To set information:

commands exec {include | exclude} all <command>

To delete information:

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

Input mode

```
(config-view)
```

Parameters

{include | exclude}

Restricts use of the specified command string.

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

all <command>

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 50 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

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

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

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

ip access-group

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

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

Syntax

To set information:

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

To delete information:

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

Input mode

```
(config-line)
```

Parameters

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <access list name>, specify a name that is no more than 31 characters.

   For details, see "Specifiable values for parameters".

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet, FTP, or SSH).
2. To permit FTP connections, set ftp-server.
3. To permit SSH connections, set ip ssh.
4. When ip access-group is not set, access using IPv4 addresses is permitted from all remote operation ter-

minals.

5. Sessions of users logging in from the IPv4 addresses that are no longer permitted due to the change will no longer be able to communicate immediately after the change.

ipv6 access-class

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

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

Syntax

To set information:

ipv6 access-class <access list name> 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 a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This setting is common to all types of remote access (Telnet, FTP, or SSH).
2. To permit FTP connections, set ftp-server.
3. To permit SSH connections, set ip ssh.
4. When ipv6 access-class is not set, access using IPv6 addresses is permitted from all remote operation terminals.
5. Sessions of users logging in from the IP addresses that are no longer permitted due to the change will be unable to communicate immediately after the change.

parser view

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

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

Syntax

To set information:

parser view <view name>

To delete information:

no parser view <view name>

Input mode

```
(config)
```

Parameters

<view name>

Specifies the name of a command list to be generated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

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

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

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

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

radius-server host

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

Syntax

To set or change information:

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

To delete information:

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

Input mode

```
(config)
```

Parameters

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

<ipv4 address>

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

<ipv6 address> [interface vlan <vlan id>]

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

Specify the interface parameter only when a link-local address is specified.

- interface vlan <vlan id>

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

<host name>

Specifies the host name of the RADIUS server with 64 or fewer characters.

For details about the characters that can be specified for the host name, see "Specifiable values for parameters".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address, an IPv6 address, or a host name can be specified.

   When an IPv6 link-local address is specified, specify the interface at the same time.

key <string>

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

1. Default value when this parameter is omitted:

   The RADIUS key set by using radius-server key is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does

not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

auth-port <port>

Specifies the RADIUS server port number.

1. Default value when this parameter is omitted:

   Port number 1812 is used.

2. Range of values:

   1 to 65535

acct-port <port>

Specifies the port number for RADIUS server accounting.

1. Default value when this parameter is omitted:

   Port number 1813 is used.

2. Range of values:

   1 to 65535

{auth-only | acct-only}

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

retransmit <retries>

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   0 to 15

timeout <seconds>

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   1 to 30

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

radius-server key

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

Syntax

To set or change information:

radius-server key <string>

To delete information:

no radius-server key

Input mode

```
(config)
```

Parameters

<string>

Specifies the RADIUS key used for encryption or for authentication of communication with the 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:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

radius-server retransmit

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

Syntax

To set or change information:

radius-server retransmit <retries>

To delete information:

no radius-server retransmit

Input mode

```
(config)
```

Parameters

<retries>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 15

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

radius-server timeout

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

Syntax

To set or change information:

radius-server timeout <seconds>

To delete information:

no radius-server timeout

Input mode

```
(config)
```

Parameters

<seconds>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 30

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

tacacs-server host

Configures the TACACS+ server used for authentication or authorization.

Syntax

To set or change information:

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

To delete information:

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

Input mode

```
(config)
```

Parameters

{<host name> | <ip address>}

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

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

key <string>

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

port <port>

Specifies the TCP port number for TACACS+ server authentication.

1. Default value when this parameter is omitted:

   Port number 49 is used.

2. Range of values:

   1 to 65535

timeout <seconds>

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   1 to 30

{auth-only | acct-only}

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

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

tacacs-server key

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

Syntax

To set or change information:

tacacs-server key <string>

To delete information:

no tacacs-server key

Input mode

```
(config)
```

Parameters

<string>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

tacacs-server timeout

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

Syntax

To set or change information:

tacacs-server timeout <seconds>

To delete information:

no tacacs-server timeout

Input mode

```
(config)
```

Parameters

<seconds>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 30

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

username

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

A maximum of 20 users can be specified per device.

Syntax

To set or change information:

username <user name> exec-timeout <minutes>

username <user name> terminal-pager {enable | disable}

username <user name> terminal-help {all | no-utility}

username <user name> view <view name>

username <user name> view-class {root | allcommand | noconfig | nomanage | noenable}

To delete information:

no username <user name>

no username <user name> exec-timeout

no username <user name> terminal-pager

no username <user name> terminal-help

no username <user name> view

no username <user name> view-class

Input mode

```
(config)
```

Parameters

<user name>

Specifies the user name to be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a string of no more than 16 characters. Alphabetic characters can be used for the first character, and alphanumeric characters, hyphens (-), and underscores (_) can be used for the second and subsequent characters.

   For exec-timeout, terminal-pager, or terminal-help, you can specify default_user, and the settings apply to all users. When default_user is specified, the settings apply only to users who are not specified using a specific user name.

exec-timeout <minutes>

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

1. Default value when this parameter is omitted:

   60

2. Range of values:

   0 to 60

terminal-pager {enable | disable}

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

enable

Paging is performed.

disable

Paging is not performed.

1. Default value when this parameter is omitted:

   enable

2. Range of values:

   None

terminal-help {all | no-utility}

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

all

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

no-utility

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

1. Default value when this parameter is omitted:

   all

2. Range of values:

   None

view <view name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

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

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

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

Specifies a command class to be assigned to a user.

Specifies any one of root, allcommand, noconfig, nomanage, and noenable command classes that have been defined in advance on the Switch.

For details, see "Configuration Guide Vol. 1, Table 8-10: Command classes".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The changed setting takes effect from the next login.

Notes

1. A maximum of 20 users including default_user can be set per device.
2. When default_user is specified, the settings apply only to users who are not specified using a specific user name. For example, when 0 is set as the exec-timeout value for default_user, if the terminal-pager or terminal-help parameter is set for the user name staff, the setting to be applied to user staff is 60, and this is set as the initial value when the exec-timeout parameter is omitted.
3. The behavior of each command can be changed temporarily just for the current log-in session by using the "set exec-timeout", "set terminal pager", or "set terminal help" operation commands after the user has logged in.

5 SSH

ip ssh

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

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

Syntax

To set information:

ip ssh

To delete information:

no ip ssh

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot log in with SSH only by setting this command. It is necessary to set the number of login users with the "line vty" command.
2. Configuration with this command and the "line vty" command enables remote access using the SSH protocol from any remote operation terminal to be accepted. To restrict access, set "ip access-group", "ipv6 access-class", or "transport input" in line vty mode.
3. Just because other SSH information commands (such as "ip ssh version") are set, the SSH server will not run unless this command is set, and therefore remote login to the Switch using SSH is not possible.

ip ssh authentication

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

Syntax

To set or change information:

ip ssh authentication {publickey | password}

To delete information:

no ip ssh authentication

Input mode

```
(config)
```

Parameters

{publickey | password}

Specify publickey to permit only public key authentication.

Specify password to permit only password authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip ssh authkey

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

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

Syntax

To set or change information:

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

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

To delete information:

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

Input mode

```
(config)
```

Parameters

<user name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   User name (No more than 16 characters)

<authentication key name>

Specifies any name for the user public key index.

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

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

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

"<public key>"

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

load-key-file <file name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

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

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

Default behavior

Login with public key authentication is not possible.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the user name for which the user public key is set with this command is not registered as an account on the Switch, the user public key will be automatically enabled when a relevant account is newly registered with the "adduser" operation command.
2. Do not create a directory named as ".ssh" under the home directory of each user. In addition, do not transfer, copy, or generate files under the ".ssh" directory.

   The ".ssh" directory is automatically generated and used by the SSH server function of the Switch. If the user puts the file there, the file will be deleted or overwritten.

ip ssh ciphers

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

Syntax

To set or change information:

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

To delete information:

no ip ssh ciphers

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

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

2. Range of values:

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

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

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

ip ssh key-exchange

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

Syntax

To set or change information:

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

To delete information:

no ip ssh key-exchange

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   The following key exchange method names can be specified:

   ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

ip ssh macs

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

Syntax

To set or change information:

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

To delete information:

no ip ssh macs

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   The following message authentication code method names can be specified:

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

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

ip ssh version

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

Syntax

To set or change information:

ip ssh version {1 | 2}

To delete information:

no ip ssh version

Input mode

```
(config)
```

Parameters

{1 | 2}

Specify 1 to permit only version 1 for connection.

Specify 2 to permit only version 2 for connection.

1. Default value when this parameter is omitted:
   This parameter cannot be omitted.
2. Range of values:
   None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

6 Time Settings and NTP

clock timezone

Sets the time zone.

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

Syntax

To set or change information:

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

To delete information:

no clock timezone

Input mode

```
(config)
```

Parameters

<zone name>

Specifies the name used to identify a time zone.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A maximum of seven alphanumeric characters

<hours offset>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<minutes offset>

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

1. Default value when this parameter is omitted:

   0

2. Range of values:

   0 to 59 (minutes)

Default behavior

UTC is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ntp access-group

Creates an access group whose access to NTP services can be permitted or denied by means of an IPv4 address filter. The maximum number of filter condition entries for an access list that can be set by using this command is 50.

Syntax

To set information:

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

To delete information:

no ntp access-group {query-only | serve-only | serve | peer}

Input mode

```
(config)
```

Parameters

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

Sets the mode in which an NTP services are used.

query-only

Only NTP control queries are permitted.

serve-only

NTP control queries and NTP broadcast messages are not permitted.

serve

NTP broadcast messages are not permitted.

peer

All accesses to NTP services are permitted.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <access list name>, specify a name that is no more than 31 characters.

   For details, see "Specifiable values for parameters".

Default behavior

All accesses to NTP services are permitted.

Impact on communication

None

When the change is applied

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

Notes

1. Implicit discard entries are invalid for access lists specified for this command.
2. If at least one access group is created, any accesses with a source IP address that does not match the specified access list are denied. If no access groups are created, all accesses are permitted.
3. When the source IP address matches access lists for multiple access types, access type keywords are applied according to the following priority:

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

ntp authenticate

Enables the NTP authentication function.

Syntax

To set information:

ntp authenticate

To delete information:

no ntp authenticate

Input mode

```
(config)
```

Parameters

None

Default behavior

The NTP authentication function is disabled.

Impact on communication

None

When the change is applied

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

Notes

None

ntp authentication-key

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

Syntax

To set or change information:

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

To delete information:

no ntp authentication-key <key id>

Input mode

```
(config)
```

Parameters

<key id>

Specifies the key number in decimal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

md5 <value>

Specifies a value to be assigned to an authentication key.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A maximum of 30 ASCII characters

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. For some destination devices, the range of available authentication keys might be less than 32 bits. In this case, set the value of a key to use to a value within the valid range of the destination device.
2. Do not specify 65536 or a larger value as the key number.

ntp broadcast

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

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

Syntax

To set or change information:

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

To delete information:

no ntp broadcast

Input mode

`(config-if)`

VLAN interface

Parameters

version <number>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

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

2. Range of values:

   1, 2, or 3

key <key id>

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

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. This function can use IPv4 only.
2. If no IPv4 addresses are set for an interface, no NTP broadcast packets are sent.
3. To change IPv4 address settings of an interface, delete the ntp broadcast setting first.
4. Do not specify 65536 or a larger value as the key number.

ntp broadcast client

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

Syntax

To set information:

ntp broadcast client

To delete information:

no ntp broadcast client

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ntp broadcastdelay

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

Syntax

To set or change information:

ntp broadcastdelay <micro seconds>

To delete information:

no ntp broadcastdelay

Input mode

```
(config)
```

Parameters

<micro seconds>

Specifies a delay time. The time is set as a decimal integer in microseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 999999

Default behavior

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

Impact on communication

None

When the change is applied

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

Notes

None

ntp master

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

Syntax

To set or change information:

ntp master [<stratum>]

To delete information:

no ntp master

Input mode

```
(config)
```

Parameters

<stratum>

Specifies the stratum value in decimal.

1. Default value when this parameter is omitted:

   8

2. Range of values:

   1 to 15

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you use the Switch as an NTP server, and 10 or more clients are to be synchronized, synchronization might be temporarily disabled. Although the Switch function is not affected even if the number of clients to be synchronized exceeds 10, consider your environment when deciding the number of clients.
2. If 16 or a larger value is set as the stratum value, the Switch assumes that the stratum value is 15.

ntp peer

Sets the active/passive mode with a symmetric connection between the specified NTP server and the Switch. By synchronizing with the specified NTP server, the Switch also works as an NTP server.

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

Syntax

To set or change information:

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

To delete information:

no ntp peer <ip address>

Input mode

```
(config)
```

Parameters

<ip address>

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

version <number>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

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

2. Range of values:

   1, 2, or 3

key <key id>

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

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

prefer

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

1. Default value when this parameter is omitted:

   No priorities are set.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the Switch and other devices are configured in symmetric active/passive mode, it might take a very long time to synchronize these devices. If this happens, we recommend that you reduce the number of devices in the configuration.
2. When a device references multiple time-reference synchronization-source devices, if the time of a high-priority synchronization-source device moves outside of the synchronization range (a 1000 second or longer time difference), other synchronization-source devices will be used as the time reference. If this situation is not fixed, synchronization with the other devices might also be lost. You can change the settings to manually disable the synchronization-source designation of the device whose time has moved out of the valid range. Another solution in this case is to manually reset the time of such a device to the correct value, and synchronization will be recovered.
3. Do not specify 65536 or a larger value as the key number.
4. If multiple NTP servers are configured in the network, the Switch synchronizes with the NTP server specified with the <prefer> parameter of the "ntp peer" command. Additionally, if the <prefer> parameter is not specified, synchronization will be performed with the NTP server with the lowest stratum value, and if all stratum values are the same, synchronization will be performed with any NTP server.

ntp server

Sets the client/server mode and specifies the client mode for the Switch. By synchronizing with the specified NTP server, the Switch also works as an NTP server.

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

Syntax

To set or change information:

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

To delete information:

no ntp server <ip address>

Input mode

```
(config)
```

Parameters

<ip address>

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

version <number>

Specifies the NTP version number.

1. Default value when this parameter is omitted:

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

2. Range of values:

   1, 2, or 3

key <key id>

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

1. Default value when this parameter is omitted:

   No authentication keys are specified.

2. Range of values:

   1 to 65535

prefer

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

1. Default value when this parameter is omitted:

   No priorities are set.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Do not specify 65536 or a larger value as the key number.
2. If multiple time servers are configured in the network, the Switch synchronizes with the time server specified with the <prefer> parameter of the "ntp server" command. Additionally, if the <prefer> parameter is not specified, synchronization will be performed with the time server with the lowest stratum value, and if all stratum values are the same, synchronization will be performed with any time server.

ntp trusted-key

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

Syntax

To set information:

ntp trusted-key <key id>

To delete information:

no ntp trusted-key <key id>

Input mode

```
(config)
```

Parameters

<key id>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

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

7 Host Names and DNS

ip domain lookup

Enables or disables the DNS resolver function.

Syntax

To set information:

no ip domain lookup

To delete information:

ip domain lookup

Input mode

```
(config)
```

Parameters

None

Default behavior

The DNS resolver function is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip domain name

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

Syntax

To set or change information:

ip domain name <domain name>

To delete information:

no ip domain name

Input mode

```
(config)
```

Parameters

<domain name>

Sets the domain name for the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

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

Notes

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

ip domain reverse-lookup

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

Syntax

To set information:

```
no ip domain reverse-lookup
```

To delete information:

```
ip domain reverse-lookup
```

Input mode

```
(config)
```

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

ip host

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

Syntax

To set or change information:

ip host <name> <ip address>

To delete information:

no ip host <name>

Input mode

```
(config)
```

Parameters

<name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<ip address>

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

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. localhost cannot be set as a host name.
2. 127.*.*.* cannot be set as an IPv4 address.
3. A class D or class E IPv4 address cannot be set.
4. Host names are not case sensitive.

ip name-server

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

Syntax

To set information:

ip name-server <ip address>

To delete information:

no ip name-server <ip address>

Input mode

```
(config)
```

Parameters

<ip address>

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

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

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

Notes

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

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

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

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

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

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

```
nslookup: can't resolve '<host name to reference>'
```

2. 127.*.*.* cannot be specified as an IP address.
3. Class D and class E addresses cannot be set as IP addresses.
4. AAAA query information cannot be referenced by using IPv6. AAAA query information is referenced by IPv4.

ipv6 host

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

Syntax

To set or change information:

ipv6 host <name> <ipv6 address>

To delete information:

no ipv6 host <name>

Input mode

```
(config)
```

Parameters

<name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<ipv6 address>

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

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. localhost cannot be set as a host name.
2. Host names are not case sensitive.
3. If the same host name is specified for the "ipv6 host" command and the "ip host" command, the "ip host" command takes priority.

8 Device Management

switch provision

Sets the device model.

Syntax

To set information:

switch <switch no.> provision {2340-16t4x | 2340-24t4x | 2340-24th4x | 2340-48t4x | 2340-24p4x | 2340-24ph4x | 2340-48p4x | 2340-16p8mp2x}

Input mode

```
(config)
```

Parameters

<switch no.>

Specifies a switch number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

{2340-16t4x | 2340-24t4x | 2340-24th4x | 2340-48t4x | 2340-24p4x | 2340-24ph4x | 2340-48p4x | 2340-16p8mp2x}

2340-16t4x

Sets the AX2340S-16T4X model.

2340-24t4x

Sets the AX2340S-24T4X model.

2340-24th4x

Sets the AX2340S-24TH4X model.

2340-48t4x

Sets the AX2340S-48T4X model.

2340-24p4x

Sets the AX2340S-24P4X model.

2340-24ph4x

Sets the AX2340S-24PH4X model.

2340-48p4x

Sets the AX2340S-48P4X model.

2340-16p8mp2x

Sets the AX2340S-16P8MP2X model.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The Switch works according to the automatically set information.

Impact on communication

None

When the change is applied

The change takes effect immediately after it is made.

Notes

None

system fan mode

Sets the operating mode of the fan.

Syntax

To set or change information:

system fan mode <mode>

To delete information:

no system fan mode

Input mode

```
(config)
```

Parameters

<mode>

Specifies operating mode 1 or 2 for the fan.

1: Low-noise setting

2: Low-temperature setting

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 and 2

Default behavior

1: The low-noise setting is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

system l2-table mode

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

Syntax

To set information:

system l2-table mode <mode>

To delete information:

no system l2-table mode

Input mode

```
(config)
```

Parameters

<mode>

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

1 to 3

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3

Default behavior

1 is set as the method for searching the table.

Impact on communication

If you set a value of 1 to 3 for the parameter, you need to restart the Switch to set the table search method for the hardware. Restarting the Switch temporarily prevents data from being sent or received.

When the change is applied

The change is applied when the Switch is restarted.

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

None

system memory-soft-error

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

Syntax

To set information:

system memory-soft-error log

To delete information:

no system memory-soft-error log

Input mode

```
(config)
```

Parameters

log

Outputs an operation message when a soft error occurs in memory inside the switch processor.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

system recovery

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

Syntax

To set information:

no system recovery

To delete information:

system recovery

Input mode

```
(config)
```

Parameters

None

Default behavior

Recovery is performed and failed parts are re-initialized.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

system temperature-warning-level

Outputs an operation message when the temperature inside the Switch reaches or exceeds the specified temperature.

Syntax

To set information:

system temperature-warning-level <temperature>

To delete information:

no system temperature-warning-level

Input mode

```
(config)
```

Parameters

<temperature>

Specifies the temperature inside the Switch (in Celsius).

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   50 to 75

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

If the temperature inside the Switch has already reached or exceeded the specified temperature, an operation message is immediately output.

9 Zero-touch Provisioning

system zero-touch-provisioning

Enables the zero-touch provisioning. This command is valid for the initial installation configuration.

Syntax

To set information:

system zero-touch-provisioning

To delete information:

no system zero-touch-provisioning

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

After changing the settings, save the configuration. Applies at the next startup of the Switch.

Notes

1. If the zero-touch provisioning is not used, delete this command.

system zero-touch-provisioning vlan

Set the VLAN to use for the zero-touch provisioning. This command can be set for only one VLAN on the Switch. In the initial configuration, a default VLAN (VLAN ID = 1) is set.

Syntax

To set or change information:

system zero-touch-provisioning vlan <vlan id>

To delete information:

no system zero-touch-provisioning vlan

Input mode

```
(config)
```

Parameters

vlan <vlan id>

Set the VLAN to use for the zero-touch provisioning.

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

After changing the settings, save the configuration. Applies at the next startup of the Switch.

Notes

None

10 Power Saving Functions

eee enable

Enables the EEE function on the following Ethernet interface.

- 10BASE-T/100BASE-TX/1000BASE-T
- 100BASE-TX/1000BASE-T/2.5GBASE-T

However, this does not include when using SFP port or SFP+/SFP shared port with 1000BASE-T.

Syntax

To set information:

eee enable

To delete information:

no eee enable

Input mode

```
(config-if)
```

Ethernet interface

Parameters

None

Default behavior

EEE function is disabled.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is enabled during auto-negotiation.
2. Enabled only when the line speed is 100BASE-TX and 1000BASE-T full duplex.

11 Log Data Output Function

logging email

Sets the email address to which log information is output as an email. This command can configure a maximum of 64 entries.

Syntax

To set information:

logging email <e-mail address>

To delete information:

no logging email <e-mail address>

Input mode

```
(config)
```

Parameters

<e-mail address>

Specifies the destination email address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   You can use only alphanumeric characters, hyphens (-), underscores (_), periods (.) and at marks (@) with no more than 255 characters.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You must use the "logging email-server" command beforehand to set the SMTP server to which an email is sent.
2. You must configure the settings related to the DNS resolver function beforehand.
3. Make sure that the specified email address matches the address set for the destination SMTP server.
4. If an attempt to send an email fails, the email is discarded.
5. If an IP address is set for the loopback interface, the IP address is used as the source IP address during communication with the SMTP server.

6. When you use an at mark (@) in an email address, do not use it for the beginning or ending of the email address. Also, do not specify multiple at marks.

logging email-event-kind

Sets the message type of log information to be output as an email. Multiple message types can be set.

Syntax

To set information:

logging email-event-kind <event kind>

To delete information:

no logging email-event-kind <event kind>

Input mode

```
(config)
```

Parameters

<event kind>

Specifies the message type for operation logs to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The message type set by using this command is applied to all destination email addresses specified by the "logging email" command.
2. If the message type is set by using this command, the default message types (evt and err) become invalid and only the message types that have been set take effect.

logging email-from

Sets the sender of log information to be output as an email.

Syntax

To set or change information:

logging email-from <e-mail address>

To delete information:

no logging email-from

Input mode

```
(config)
```

Parameters

<e-mail address>

Specifies the source email address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   You can use only alphanumeric characters, hyphens (-), underscores (_), periods (.) and at marks (@) with no more than 255 characters.

Default behavior

The sender of the email is "device-name<nobody>", where device-name is the name specified by the "hostname" command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The sender of the email set by using this command is applied to all destination email addresses specified by the "logging email" command.
2. When you use an at mark (@) in an email address, do not use it for the beginning or ending of the email address. Also, do not specify multiple at marks.

logging email-interval

Sets the sending interval for emailing output log information.

Syntax

To set or change information:

logging email-interval <seconds>

To delete information:

no logging email-interval

Input mode

```
(config)
```

Parameters

<seconds>

Specifies the email sending interval.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600 (seconds)

Default behavior

The email sending interval is set to "1".

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

logging email-server

Sets the SMTP server information for outputting log information as an email. This command can configure a maximum of 16 entries.

Syntax

To set information:

logging email-server {<host name> | <ip address>} [port <port number>]

To delete information:

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

Input mode

```
(config)
```

Parameters

{<host name> | <ip address>}

Specifies the host name or IP address of the SMTP server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <host name>

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

   <ip address>

   Specifies the IPv4 address in dot notation.

port <port number>

Specifies the SMTP server port number.

1. Default value when this parameter is omitted:

   25

2. Range of values:

   0, or 1 to 65535

   If 0 is specified, the default value when this parameter is omitted is used.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Make sure that the specified SMTP server information (the host name or IP address, and port number) matches the one set for the destination SMTP server. If the connection to the SMTP server fails while an email is being sent, the email is discarded.
2. This function can use IPv4 only. Therefore, if you specify as the SMTP server the name of a host that has only an IPv6 address set by using the "ipv6 host" command, emails sent to the server will be discarded.
3. localhost cannot be set as a host name.
4. Host names are not case sensitive.
5. 127.*.*.* cannot be set as an IPv4 address.
6. A class D or class E address cannot be specified as an IPv4 address.
7. If large amounts of log information are generated at one time, some of the information might be missing from the log emails.

logging event-kind

Sets the message type of the log information to be sent to the syslog server. Multiple message types can be set.

Syntax

To set information:

logging event-kind <event kind>

To delete information:

no logging event-kind <event kind>

Input mode

```
(config)
```

Parameters

<event kind>

Specifies the message type for operation logs to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The message type set by using this command is applied to all output destinations specified by the "logging host" command.
2. If the message type is set by using this command, the default message types (evt and err) become invalid and only the message types that have been set take effect.

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

This setting is used if a facility for each destination is specified with the <facility> parameter of the "logging host" command.

In other cases, the facility will be "local0".

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.

logging host

Sets the output destination for log information. The command can configure up to 20 entries.

Syntax

To set information:

logging host { <host name> | <ip address> | <ipv6 address>} [no-date-info] [version <version id>] [facility <facility>] [severity <level>]

To delete information:

no logging host { <host name> | <ip address> | <ipv6 address>}

Input mode

```
(config)
```

Parameters

{ <host name> | <ip address> | <ipv6 address>}

Specifies an IPv4 or IPv6 address to which log information is to be output.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <host name>, specify a host name with no more than 64 characters. For details about the characters that can be specified, see "Specifiable values for parameters".

   For <ip address>, specify the IPv4 address in dot notation.

   For <IPv6-Address>, specify the IPv6 address in colon notation.

no-date-info

Sends the information after excluding the time from log information.

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

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

1. Default value when this parameter is omitted:

   All log information is sent.

2. Range of values:

   None

version <version id>

Sets the syslog format version. If 1 is specified for <version id>, sends the syslog message in the format compliant with RFC 5424.

If this parameter is specified, it takes precedence over the setting of the "logging syslog-version" command.

1. Default value when this parameter is omitted:

   Sends the syslog message in the format compliant with RFC 3164.

2. Range of values:

1

facility <facility>

Sets a facility to which log information is output via the syslog interface. If this parameter is specified, it takes precedence over the setting of the "logging facility" command.

1. Default value when this parameter is omitted:

   Follows the settings of the "logging facility" command.

2. Range of values:

   See the <facility> parameter of the "logging facility" command.

severity <level>

Sets the level of importance for log information to be sent to the syslog server. If this parameter is specified, it takes precedence over the setting of the "logging trap" command.

1. Default value when this parameter is omitted:

   Follows the settings of the "logging trap" command.

2. Range of values:

   See the <level> or <keyword> parameter of the "logging trap" command.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To use the syslog function, a syslog daemon program must be running on the destination host and the host must be configured so that it can receive the syslog information from the Switch.
2. If an IP address is set for the loopback interface, the IP address is used as the source IP address from which syslog information is sent.
3. localhost cannot be specified as a host name.
4. Host names are not case sensitive.
5. 127.*.*.* cannot be set as an IPv4 address.
6. A class D or class E IPv4 address cannot be set.
7. IPv6 addresses can be global addresses.
8. If a large amount of log information is generated at one time, some information might be missing from the syslog information.
9. Even if no-date-info is specified, time information remains in the log information saved in the device.
10. If no-date-info is specified, time information is excluded from the body of the message sent to the log output destination. However, because the log data output function adds time information to the message header, the date and time when the log information was sent are displayed in the message at the log output destination.

logging syslog-dump

Configures the settings so that log data generated on a device is not stored in the internal flash memory.

Syntax

To set information:

```
no logging syslog-dump
```

To delete information:

```
logging syslog-dump
```

Input mode

```
(config)
```

Parameters

None

Default behavior

Log data is stored in the internal flash memory.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Log data mentioned here includes operation logs (/usr/var/log/system.log) and reference logs (/usr/var/log/error.log).
2. We recommend that you send log data via the syslog interface because this setting does not store log data in the Switch.
3. Even if this setting has been configured, the startup log data and the log data for the cause of the startup that is output when the Switch starts is saved in the internal flash memory.
4. Executing the "clear logging" operation command accesses the internal flash memory and erases the log data.

logging syslog-version

Sets the format version of the syslog message sent to the syslog server.

Syntax

To set information:

logging syslog-version <version id>

To delete information:

no logging syslog-version

Input mode

```
(config)
```

Parameters

<version id>

Sets the syslog format version. If 1 is specified for <version id>, sends the syslog message in the format compliant with RFC 5424.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1

Default behavior

This setting is used if a format version for each destination is specified with the <version> parameter of the "logging host" command.

Otherwise, sends the syslog message in the format compliant with RFC 3164.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

logging trap

Sets the level of importance for log information to be sent to the syslog server.

Syntax

To set or change information:

logging trap { <level> | <keyword> }

To delete information:

no logging trap

Input mode

```
(config)
```

Parameters

{ <level> | <keyword> }

Select either a level or a keyword as the priority of syslog messages.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   Table 11-1: Priorities that can be specified

Level	Keyword	Description
0	emergencies	System unavailable
1	alerts	Immediate action required
2	critical	Critical state
3	errors	Error state
4	warnings	Warning state
5	notifications	Normal but attention required
6	information	Messages that are intended for notification only
7	debugging	Message displayed during debugging only

Default behavior

This setting is used if a priority for each destination is specified with the <severity> parameter of the "logging host" command.

Otherwise, "information" (priority level 6) is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

12 SNMP

hostname

Sets the identification name of a Switch.

Syntax

To set or change information:

hostname <name>

To delete information:

no hostname

Input mode

```
(config)
```

Parameters

<name>

The identification name of a Switch. Set a name that is unique in the network that will be used. This information can be referenced by using the name set in [sysName] in the system group for enquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the Set operation of SNMP. If this name is changed by the Set operation of SNMP, the name is applied to the configuration. This parameter is equivalent to sysName defined in RFC 1213.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

No identification name is initially set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about name, contact, and location from the SNMP manager, you must use the "snmp-server community" command to register the SNMP manager.

rmon alarm

Sets the control information of the RMON (RFC 1757) alarm group. This command can configure a maximum of 128 entries.

Syntax

To set or change information:

rmon alarm <number> <variable> <interval> {delta | absolute} rising-threshold <value> rising-event-index <event no.> falling-threshold <value> falling-event-index <event no.> [owner string] [start-up_alarm { rising_falling | rising | falling }]

To delete information:

no rmon alarm <number>

Input mode

```
(config)
```

Parameters

<number>

Specifies the information identification number for the RMON alarm group control information. This parameter is equivalent to alarmIndex defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

<variable>

Specifies the object identifier for the MIB used for checking the threshold. This parameter is equivalent to alarmVariable defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a MIB object identifier (in dot format) in double quotation marks ("). Only object identifiers that can be specified in no more than 63 characters are valid. Specify the Integer, TimeTicks, Counter, or Gauge type of the object identifier. If an input character string does not include special characters other than alphanumeric characters and periods (.), you do not have to enclose the character string in double quotation marks (").

<interval>

Specifies the time interval (in seconds) for checking the threshold. This parameter is equivalent to alarmInterval defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4294967295

{ delta | absolute }

Specifies the threshold check method. If delta is specified, the difference between the current value and the value of the last sampling is compared with the threshold. If absolute is specified, the current value is compared directly with the threshold. This parameter is equivalent to alarmSampleType defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

rising-threshold <value>

Specifies the upper threshold. This parameter is equivalent to alarmRisingThreshold defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   -2147483648 to 2147483647

rising-event-index <event no.>

Specifies the identification number of the method for generating an event if the upper threshold is exceeded. The method for generating an event is the information identification number for the control information specified by using the "event" configuration command. This parameter is equivalent to alarmRisigEventIndex defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An information identification number from 1 to 65535 for the control information specified by using the "event" configuration command for <event no.>

falling-threshold <value>

Specifies the lower threshold value. This parameter is equivalent to alarmFallingThreshold defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   -2147483648 to 2147483647

falling-event-index <event no.>

Specifies the identification number of the method for generating an event if the lower threshold is exceeded. The method for generating an event is the information identification number for the control information specified by using the "event" configuration command. This parameter is equivalent to alarmFallingEventIndex defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An information identification number from 1 to 65535 for the control information specified by using the "event" configuration command for <event no.>

owner <string>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter is equivalent to alarmOwner defined in

RFC 1757.

1. Default value when this parameter is omitted:

   NULL

2. Range of values:

   Enclose a character string of no more than 24 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

startup_alarm { rising_falling | rising | falling }

Specifies the timing for checking the threshold in the first sampling. If rising is specified, an alarm is generated when the upper threshold is exceeded in the first sampling. If falling is specified, an alarm is generated when a value drops below the lower threshold in the first sampling. If rising_falling is specified, an alarm is generated when the upper or lower threshold is crossed in the first sampling. This parameter is equivalent to alarmstartUpAlarm defined in RFC 1757.

1. Default value when this parameter is omitted:

   rising_falling

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To access an alarm group from the SNMP manager, you must register the SNMP manager by using the "snmp-server community" command.
2. As the value for rising-event-index or falling-event-index of an alarm group, set the information identification number for an event group that has been set in the switch configuration.
3. A maximum of 128 entries can be set for the alarm groups set in the configuration and set from the SNMP manager by using the Set operation of SNMP. When the maximum number of entries have been set, even if an alarm group is set in the configuration, the added alarm group will not work. Delete unnecessary alarm settings, and then reconfigure the alarm settings.
4. If the Set operation is performed from the SNMP manager for RMON alarmTable, the result of the operation will not be applied to the configuration.
5. Some alarms might not work if they cannot collect MIB information, such as when there are too many alarm configurations or when the value set for the interval is 60 seconds or less. In such a case, the MIB value for alarmStatus is invalid(4). If this happens, change the interval value to 60 seconds or larger, or delete unnecessary alarm settings.
6. If the set interval value is too large, valid(1) is returned for the time being until alarmStatus changes from valid(1) to invalid(4) for a reason described in 5. above or other reasons (as a guide, it takes time of about half of the interval value).

rmon collection history

Configure the control information for the RMON (RFC 1757) Ethernet statistics history.

Syntax

To set or change information:

rmon collection history controlEntry <integer> [owner <owner name>] [buckets <bucket number>] [interval <seconds>]

To delete information:

no rmon collection history controlEntry <integer>

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<integer>

Specifies the information identification number for the statistics history control information. This parameter is equivalent to historyControlIndex defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

owner <owner name>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter is equivalent to historyControlOwner defined in RFC 1757.

1. Default value when this parameter is omitted:

   Blank

2. Range of values:

   Enclose a character string of no more than 24 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

buckets <bucket number>

Specifies the number of history entries in which statistics can be stored. This parameter is equivalent to historyControlBucketsRequested defined in RFC 1757.

1. Default value when this parameter is omitted:

   50

2. Range of values:

   1 to 65535

   Note: If a value from 51 to 65535 is specified for <bucket number>, the behavior is the same as if

50 had been specified.

interval <seconds>

Specifies the time interval (in seconds) for collecting statistics. This parameter is equivalent to historyControlInterval defined in RFC 1757.

1. Default value when this parameter is omitted:

   1800

2. Range of values:

   1 to 3600

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To access an Ethernet history group from the SNMP manager, you must register the SNMP manager by using the "snmp-server community" command.
2. A maximum of 32 entries can be set for the history groups set in the configuration and set from the SNMP manager by using the Set operation of SNMP. When the maximum number of entries have been set, even if a history group is set in the configuration, the added history group will not work. Delete unnecessary history settings, and then reconfigure the history settings.
3. If the Set operation is performed from the SNMP manager for RMON historyControlTable, the result of the operation will not be applied to the configuration.

rmon event

Sets the control information for the RMON (RFC 1757) event group. This command can configure a maximum of 16 entries.

Syntax

To set or change information:

rmon event <event no.> [log] [trap <community>] [description <string>] [owner <string>]

To delete information:

no rmon event <event no.>

Input mode

```
(config)
```

Parameters

<event no.>

Specifies the information identification number for the control information for an RMON event group. This parameter is equivalent to eventIndex defined in RFC 1757.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

log

This parameter specifies the method for generating an alarm (event) and generates an alarm log. This parameter is equivalent to eventType defined in RFC 1757.

1. Default value when this parameter is omitted:

   An alarm log is not generated.

2. Range of values:

   None

trap <community>

This parameter specifies the method for generating an alarm (event) and sends SNMP notifications to the community specified for <community>. This parameter is equivalent to eventType defined in RFC 1757.

1. Default value when this parameter is omitted:

   SNMP notifications are not sent.

2. Range of values:

   For <community>, enclose a character string consisting of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

description <string>

Uses a character string to specify the description of an event. Use this parameter as a note regarding the event. This parameter is equivalent to eventDescription defined in RFC 1757.

1. Default value when this parameter is omitted:

   Blank

2. Range of values:

   Enclose a character string of no more than 79 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

owner <string>

Specifies the identification information of the person who specified this setting. This information is used to identify the person who specified this setting. This parameter is equivalent to eventOwner defined in RFC 1757.

1. Default value when this parameter is omitted:

   Blank

2. Range of values:

   Enclose a character string of no more than 24 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When an event group is accessed from the SNMP manager and SNMP notifications are sent to the SNMP manager, you must register the SNMP manager by using the "snmp-server community" and "snmp-server host" commands.
2. To send SNMP notifications to the SNMP manager, specify the IP address of the destination SNMP manager and "rmon" by using the "snmp-server host" command.
3. An SNMP notification is sent only if the community name used when the SNMP manager is registered matches the community name of the event group.
4. As the value for rising-event-index or falling-event-index of an alarm group, set the information identification number that has been set for the corresponding event group. If the values are different, no event is executed when an alarm is generated.
5. A maximum of 16 entries can be set for the event groups set in the configuration and set from the SNMP manager by using the Set operation of SNMP. When the maximum number of entries have been set, even if an event group is set in the configuration, the added event group will not work. Delete unnecessary event settings, and then reconfigure the event settings.
6. If the Set operation is performed from the SNMP manager for RMON eventTable, the result of the operation will not be applied to the configuration.

snmp-server community

Sets the access list for the SNMP community. A maximum of 50 addresses can be registered by this command.

Syntax

To set or change information:

snmp-server community <community> [{ ro | rw }] [{<access list number> | <access list name>}]

To delete information:

no snmp-server community <community>

Input mode

```
(config)
```

Parameters

<community>

Sets the community name for the SNMP manager.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

{ ro | rw }

For the manager that has the specified IP address belonging to the community with the specified community name, sets a functional mode for the manager to handle MIB-related information. If ro is specified, Get Request and GetNext Request are permitted. If rw is specified, Get Request, GetNext Request, and Set Request are permitted.

1. Default value when this parameter is omitted:

   ro

2. Range of values:

   None

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

Specifies the number or name of the access list in which the permissions for this community are set. If the specified {<access list number> | <access list name>} has not been set, all accesses are permitted.

One access list is permitted for one community.

1. Default value when this parameter is omitted:

   All accesses are permitted.

2. Range of values:

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

   For <access list name>, specify a name that is no more than 31 characters.

For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Creates the following entry in the snmpVacmMIB group.
   - vacmSecurityName: Community name#
   - vacmGroupName: $community (fixed value)
   - vacmViewTreeFamilyViewName: $all (fixed value)

   Also, if one or more of this command is set, an entry with vacmSecurityName as $private is created for the "snmp get" operation command. Cannot be used for access from outside the Switch.

   #

   Up to 32 characters. If it is 33 characters or more, it will be $sec00 (numbers will be assigned unique values).

snmp-server contact

Sets the contact information of the Switch.

Syntax

To set or change information:

snmp-server contact <contact>

To delete information:

no snmp-server contact

Input mode

(config)

Parameters

<contact>

Sets the contact information for the Switch used when a failure occurs on the Switch. This information can be referenced by using the name set in [sysContact] of the system group for inquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the Set operation of SNMP. If this name is changed by the Set operation of SNMP, the name is applied to the configuration. This parameter is equivalent to sysContact defined in RFC 1213.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The initial value is null.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about name, contact, and location from the SNMP manager, you must use the "snmp-server community" command to register the SNMP manager.

snmp-server engineID local

Sets SNMP engine ID information.

Syntax

To set or change information:

snmp-server engineID local <engineid string>

To delete information:

no snmp-server engineID local

Input mode

```
(config)
```

Parameters

<engineid string>

Sets an SNMP engine ID.

The SNMP engine ID value set for a device is as follows:

1st to 4th octets: A value obtained by the OR bit of an enterprise code and 0x80000000

5th octet: Fixed value of 4

6th to 32nd octets: Setting value for <engineid string>

Use the "snmp" operation command to check the SNMP engine ID to be set for a device. An example is as follows.

```
> snmp get snmpEngineID.0
Name: snmpEngineID.0
Value:80 00 FF FF 04 73 6E 6D 70 5F 54 6F 6B 79 6F 31
```

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 27 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The SNMP engine ID value set for a device is as follows:

1st to 4th octets: A value obtained by the OR bit of an enterprise code and 0x80000000

5th octet: Fixed value of 128

6th to 9th octets: A random number

10th to 13th octets: Universal timer value when the ID is automatically generated

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If many users (a maximum of 50 users) are set by using the "snmp-server user" command, setting, changing, or deleting the "snmp-server engineID local" command takes a maximum of 20 seconds.

snmp-server group

Sets SNMP security group information. Security level information and access control information consisting of the SNMP view information set by the "snmp-server view" command are grouped. A maximum of 50 group names can be set by this command.

Syntax

To set or change information:

snmp-server group <group name> v3 {noauth | auth | priv} [read <view name>] [write <view name>] [notify <view name>]

To delete information:

no snmp-server group <group name> v3 { noauth | auth | priv }

Input mode

```
(config)
```

Parameters

<group name>

Configures an SNMP security group name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

{ noauth | auth | priv }

Sets the security level of access control. When an SNMP packet is received, processing checks whether the received packet matches the security level set by this parameter. When an SNMP packet is sent, the SNMP packet is generated with the security level set by this parameter.

noauth: Authentication and encryption are not required.

auth: Authentication is required, and encryption is not required.

priv: Authentication and encryption are both required.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

read <view name>

Sets the read view name for access control. When an SNMP packet with any of the following PDU types is received, if the read view name specified for <view name> exists in the SNMP MIB view information, the MIB view is checked:

- GetRequest-PDU

- GetNextRequest-PDU
- GetBulkRequest-PDU

1. Default value when this parameter is omitted:

   The read access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

write <view name>

Sets the write view name of access control. When an SNMP packet with the SetRequest-PDU PDU type is received, if the write view name specified for <view name> exists in the SNMP MIB view information, the MIB view is checked.

1. Default value when this parameter is omitted:

   The write access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

notify <view name>

Sets the notify view name of access control. When a trap (an SNMP packet with the SNMPv2-Trap-PDU PDU type) is sent, if the notify view name specified for <view name> exists in the SNMP MIB view information, the MIB view is checked.

1. Default value when this parameter is omitted:

   The notify access permission is not granted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a MIB view name that has not been set by the "snmp-server view" command is set for the read view name, write view name, or notify view name of this command, the view name information set by this command is invalid.

snmp-server host

Registers the destination network management device (SNMP manager) to which SNMP notifications are sent. This command can configure a maximum of 4 entries.

Syntax

To set or change information:

snmp-server host <manager address> { traps | informs } <string> [version { 1 | 2c | 3 { noauth | auth | priv } }] [snmp] [rmon] [air-fan] [power] [login] [memory] [system-msg] [temperature] [frame_error_snd] [frame_error_rcv] [storm-control] [efmoam] [loop-detection] [cfm] [switchport-backup] [lldp] [poe]

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).

{traps | informs}

Sets the type of SNMP notifications that will be sent to the SNMP manager.

- If traps is specified, traps will be sent. The SNMP manager does not send a response.
- If informs is specified, informs will be sent. Because an inform requests the SNMP manager to send a response, the SNMP agent monitors for a response. If no response is returned, the inform is resent. This parameter can be used only in version SNMPv2C.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<string>

For SNMPv1 and SNMPv2C, this parameter sets the community name for the SNMP manager. For SNMPv3, this parameter sets the security user name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string

in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

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

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

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

Table 12-1: Correspondence between the parameter value and SNMP notification version

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

Legend: —: Not applicable

1. Default value when this parameter is omitted:

   version 1

2. Range of values:

   None

[snmp] [rmon] [air-fan] [power] [login] [memory] [system-msg] [temperature] [frame_error_snd] [frame_error_rcv] [storm-control] [efmoam] [loop-detection] [cfm] [switchport-backup] [lldp] [poe]

Select the SNMP notification to send by setting each parameter. The following table shows the SNMP notifications sent when each parameter is set.

Table 12-2: Correspondence between the parameter value and SNMP notification version

Parameter	SNMP notifications
snmp	coldStart
	warmStart
	linkUp
	linkDown
	authenticationFailure
rmon	risingAlarm
	fallingAlarm
air-fan	axsAirFanStopTrap
power	axsPowerSupplyFailureTrap

Parameter	SNMP notifications
login	axsLoginSuccessTrap
	axsLoginFailureTrap
	axsLogoutTrap
memory	axsMemoryUsageTrap
system-msg	axsSystemMsgTrap
temperature	axsTemperatureTrap
frame_error_snd	axsFrameErrorSendTrap
frame_error_rcv	axsFrameErrorReceiveTrap
storm-control	axsBroadcastStormDetectTrap
	axsMulticastStormDetectTrap
	axsUnicastStormDetectTrap
	axsBroadcastStormPortInactivateTrap
	axsMulticastStormPortInactivateTrap
	axsUnicastStormPortInactivateTrap
	axsBroadcastStormRecoverTrap
	axsMulticastStormRecoverTrap
	axsUnicastStormRecoverTrap
efmoam	axsEfmoamUdldPortInactivateTrap
	axsEfmoamLoopDetectPortInactivateTrap
loop-detection	axsL2ldLinkDown
	axsL2ldLinkUp
	axsL2ldLoopDetection
cfm	dot1agCfmFaultAlarm
switchport-backup	axsUlrChangeSecondary
	axsUlrChangePrimary
	axsUlrActivePortDown
lldp	lldpV2RemTablesChange
poe	pethPsePortOnOffNotification
	pethMainPowerUsageOnNotification
	pethMainPowerUsageOffNotification

snmp

Sends SNMP notifications for coldStart, warmStart, linkDown, linkUp, and authenticationFailure.

rmon

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

air-fan

Sends an SNMP notification when a fan stops.

power

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

login

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

memory

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

system-msg

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

temperature

Sends an SNMP notification when the temperature status is changed.

frame_error_snd

Sends an SNMP notification when a frame sending error occurs.

frame_error_rcv

Sends an SNMP notification when a frame reception error occurs.

storm-control

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

efmoam

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

loop-detection

Sends an SNMP notification when a L2 loop is detected.

cfm

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

switchport-backup

Sends SNMP notifications for uplink redundancy.

lldp

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

poe

Sends an SNMP notification when the power status changes or the total power consumption of a Switch exceeds the threshold.

1. Default value when this parameter is omitted:

   SNMP notifications are not sent for the parameter.

2. Range of values:

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When 3 has been set for the version, if a security user name that has not been set in the "snmp-server user" command is set by this command, the security user information set in this command is invalid.
2. If the version is set to 3 and a security level higher than the security level of the security user specified in <string> is set, it is disabled.
3. "poe" can be set only on models that support the PoE function.

snmp-server informs

Sets the conditions for sending informs. This setting is valid for SNMP managers for which the informs parameter of the "snmp-server host" command is set.

Syntax

To set or change information:

snmp-server informs [retries <retries>] [timeout <seconds>] [pending <pending>]

Note: At least one parameter must be specified.

To delete information:

no snmp-server informs

Input mode

```
(config)
```

Parameters

retries <retries>

Sets the maximum number of times an inform can be resent to the SNMP manager. If 0 is set, resending is not performed.

1. Default value when this parameter is omitted:

   3

2. Range of values:

   0 to 100

timeout <seconds>

Sets the timeout time in seconds for informs to the SNMP manager.

1. Default value when this parameter is omitted:

   30

2. Range of values:

   1 to 1800

pending <pending>

Sets the maximum number of inform that the Switch can retain at the same time.

The inform is retained until there is a response from the SNMP manager or until the timeout occurs when there are no retransmissions left, but if the maximum number is exceeded, the inform is discarded without being retransmitted at the timeout. It may appear that the maximum number has been exceeded temporarily until the opportunity to resend occurs.

1. Default value when this parameter is omitted:

   25

2. Range of values:

   1 to 4500

Default behavior

The initial values for all parameters of this command are used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

snmp-server location

Sets the name of the location where the Switch is installed.

Syntax

To set or change information:

snmp-server location <location>

To delete information:

no snmp-server location

Input mode

```
(config)
```

Parameters

<location>

Sets the name of the location where the Switch is installed. This information can be referenced by using the name set in [sysLocation] of the system group for inquiries from the SNMP manager. This name can also be changed from the SNMP manager by using the Set operation of SNMP. If this name is changed by the Set operation of SNMP, the name is applied to the configuration. This parameter is equivalent to sysLocation defined in RFC 1213.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 60 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The initial value is null.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To reference information about name, contact, and location from the SNMP manager, you must use the "snmp-server community" command to register the SNMP manager.

snmp-server traps

Sets when to send an SNMP notification.

Syntax

To set or change information:

snmp-server traps [{ limited_coldstart_trap | unlimited_coldstart_trap }] [link_trap_bind_info { private | standard }] [system_msg_trap_level <level>] [agent-address <agent address>]

To delete information:

no snmp-server traps

Input mode

```
(config)
```

Parameters

{ limited_coldstart_trap | unlimited_coldstart_trap }

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

Table 12-3: Triggers causing coldStart to be sent for each parameter

Parameter	Triggers causing coldStart to be sent
limited_coldstart_trap	• When a device starts
unlimited_coldstart_trap	• When a device starts • When the IP address of a VLAN is added, deleted, or changed due to a change in the configuration • When the time is changed by using the "set clock" command

1. Default value when this parameter is omitted:

   limited_coldstart_trap

2. Range of values:

   None

link_trap_bind_info {private | standard}

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

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

Table 12-4: TMIBs to be added when a link trap is sent, for each parameter

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

1. Default value when this parameter is omitted:

   standard

2. Range of values:

None

system_msg_trap_level <level>

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

Table 12-5: Setting value and its target event level severity

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

1. Default value when this parameter is omitted:

   9

2. Range of values:

   1 to 9

agent-address <agent address>

Specifies the IPv4 address to be used for the agent address in a trap notification frame in SNMPv1 format. Because only the SNMPv1 frame format can have the agent address field in Trap-PDUs, the address set by using this command is applied to SNMPv1 traps.

1. Default value when this parameter is omitted:

   When this parameter has not been set, if an IPv4 address has been set for interface loopback, that address is used for the agent address. If such an address has not been set, the IPv4 address for the interface that has the lowest ifIndex is used as the agent address in a trap notification frame. The target interface is VLAN. If no IPv4 address has been set for the device, 0.0.0.0 is used.

2. Range of values:

   Specify an IPv4 address from 0.0.0.0 to 255.255.255.255 for <agent address>.

Default behavior

The initial values for all parameters of this command are used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

snmp-server user

Sets SNMP security user information. The user information created by this command is to be used in the "snmp-server group" command and the "snmp-server host" command. This command can configure a maximum of 50 entries.

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

Table 12-6: Combination of the authentication protocol and the privacy protocol

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

Syntax

To set or change information:

snmp-server user <user name> <group name> v3 [auth { md5 | sha | sha256 | sha512 } <authentication password> [priv { des | aes128 } <privacy password>]]

To delete information:

no snmp-server user <user name>

Input mode

```
(config)
```

Parameters

<user name>

Configures an SNMP security user name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

<group name>

Sets the name of the SNMP security group to which the SNMP security user belongs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

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

auth { md5 | sha | sha256 | sha512 } <authentication password>

Specifies the authentication protocol and the authentication password.

md5: HMAC-MD5 is used for the authentication protocol.

sha: HMAC-SHA1 is used for the authentication protocol.

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

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

priv { des | aes128 } <privacy password>

Specifies the privacy protocol and the privacy password.

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

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

1. Default value when this parameter is omitted:

   If auth and subsequent parameter options are omitted, an authentication protocol will not be used.

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

2. Range of values:

   For <authentication password> and <privacy password>, set a character string consisting of 8 to 32 characters, enclosed in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a security group name that has not been set by the "snmp-server group" command is set in this command, the security group information set in this command will be invalid.

snmp-server view

Sets MIB view information. The MIB view information is used to check the object ID for Variable Bindings contained in SNMP PDUs. The MIB view consists of one subtree or multiple subtrees. A subtree is set by the combination of the object ID and view type. The MIB view created by this command is to be used in the "snmp-server group" command.

The following table lists the number of entries for each parameter that can be set in this command.

Table 12-7: Number of entries for each parameter

No.	Parameter	Maximum number of entries
1	MIB view	50 entries per device
2	Subtree	30 entries per MIB view
3		500 entries per device

Syntax

To set or change information:

snmp-server view <view name> <oid tree> { included | excluded }

To delete information:

no snmp-server view <view name> <oid tree>

Input mode

```
(config)
```

Parameters

<view name>

Sets a MIB view name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

<oid tree>

Sets an object ID that indicates a subtree.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an object ID in dot notation. You can use no more than 64 characters. You can also use a wildcard (*) for each sub-ID (numbers separated by a period).

{ included | excluded }

Sets the inclusion or exclusion of a subtree. Specify included to include the subtree in the MIB view. Specify excluded to exclude the subtree from the MIB view.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When you change or delete information, if a wildcard (*) is specified for a sub-ID for <oid tree>, this entry is regarded as the same as the entry for which the sub-ID of the same position is 0. Also, if you set 0 for a sub-ID, this entry is regarded as the same as the entry for which the sub-ID of the same position is a wildcard (*).

   Therefore, if you change information for one entry, information of another entry is also overwritten. If you delete information for one entry, information of another entry is also deleted.

   Example:

```
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.0.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# snmp-server view "READ_VIEW" 1.*.1.1 included
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.*.1.1 included
snmp-server view "READ_VIEW" 1.1.1.1 excluded
(config)# no snmp-server view "READ_VIEW" 1.0.1.1
(config)# show snmp-server
snmp-server view "READ_VIEW" 1.1.1.1 excluded
```

snmp trap link-status

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

Syntax

To set information:

```
no snmp trap link-status
```

To delete information:

```
snmp trap link-status
```

Input mode

```
(config-if)
```

Ethernet interface

Parameters

None

Default behavior

SNMP notifications are not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

13 Advanced Script

aaa authorization commands script

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

Syntax

To set or change information:

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

To delete information:

no aaa authorization commands script

Input mode

```
(config)
```

Parameters

{username <user name> | bypass}

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

username <user name>

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

bypass

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <user name>, enclose a character string consisting of no more than 16 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. However, a hyphen (-) cannot be specified as the first character. If an input character string does not include any special characters, you do not have to enclose the character string in double quotation marks (").

   For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

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

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

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

- When the "aaa authorization commands" command is set

  All commands cannot be executed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The "aaa authorization commands script" command alone is not sufficient for command authorization. You also need to set the "aaa authorization commands" command. Also, command authorization by the RADIUS server is not supported. You need to configure command authorization by a TACACS+ server or locally.
2. When a Python script is started from an operation terminal via console connection (RS232C), the setting of the "aaa authorization commands console" command determines the command authorization behavior.
   - When the "aaa authorization commands console" command is not set

     Command authorization is not performed. All commands can be executed.
   - When the "aaa authorization commands console" command is set

     Command authorization is performed. However, if the bypass parameter is set, command authorization is not performed. All commands can be executed.
3. When command authorization information (command class and command list) cannot be acquired, any commands cannot be executed.

action

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

Syntax

To set information:

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

To delete information:

no action <sequence>

Input mode

```
(config-applet)
```

Parameters

<sequence>

Specifies the ascending order in which actions are performed.

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8

python <file name>

Specifies a script file to be started.

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a string of no more than 99 characters including the extension (either ".py", ".pyc", or ".pyo").

   Characters that can be used are alphanumeric characters, dots (.), hyphens (-), underscores (_), tildes (~), and hats (^).

<args>...

Specifies command line arguments to be given to the script.

1. Default value when this parameter is omitted:

   None

2. Range of values:

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

   Specifiable characters are alphanumeric characters and special characters. If you specify multiple <args>, specify them separating each with a space. If you use special characters such as a space in an <args>, enclose the string of the <args> in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you change the configuration related to a relevant applet while an action is running, the action will be executed until the end, but actions that have not been executed will not be executed.

disable

Suppresses the target applet function.

Syntax

To set information:

disable

To delete information:

no disable

Input mode

```
(config-applet)
```

Parameters

None

Default behavior

The applet is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

event manager applet

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

Syntax

To set information:

event manager applet <applet name>

To delete information:

no event manager applet <applet name>

Input mode

```
(config)
```

Parameters

<applet name>

Specifies an applet name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   Up to 256 applets can be registered.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

event sysmsg

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

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

Syntax

To set or change information:

event sysmsg [message-type <message type>] [switch <switch no.>] [event-level <event level>] [recovery-event-level <event level>] [event-function <event function> [interface-id <interface id>]] [message-id <message id>] [message-text <message text>] [additional-info-upper <upper number>] [additional-info-lower <lower number>]

One of the above monitoring condition parameters must be specified.

To delete information:

no event sysmsg

Input mode

```
(config-applet)
```

Parameters

message-type <message type>

Specifies the message type.

1. Default value when this parameter is omitted:

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

2. Range of values:

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

switch <switch no.>

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

1. Default value when this parameter is omitted:

   All switches are monitored.

2. Range of values:

   See "Specifiable values for parameters".

event-level <event level>

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

1. Default value when this parameter is omitted:

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

2. Range of values:

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

recovery-event-level <event level>

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

1. Default value when this parameter is omitted:

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

2. Range of values:

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

event-function <event function>

Specifies an event location.

1. Default value when this parameter is omitted:

   All locations and functions where an event occurred are monitored.

2. Range of values:

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

interface-id <interface id>

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

1. Default value when this parameter is omitted:

   All interface IDs are monitored.

2. Range of values:

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

message-id <message id>

Specifies the message ID.

1. Default value when this parameter is omitted:

   All message IDs are monitored.

2. Range of values:

   Specify a hexadecimal number of 8 digits or less.

message-text <message text>

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

1. Default value when this parameter is omitted:

   All message texts are monitored.

2. Range of values:

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

additional-info-upper <upper number>

Specifies the upper 4 digits of additional information.

1. Default value when this parameter is omitted:

   All the upper 4 digits of additional information are monitored.

2. Range of values:

   Specify a hexadecimal number of 4 digits or less.

additional-info-lower <lower number>

Specifies the lower 12 digits of additional information.

1. Default value when this parameter is omitted:

   All the lower 12 digits of additional information are monitored.

2. Range of values:

   Specify a hexadecimal number of 12 digits or less.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting information with this command, at least one of monitoring condition parameters must be specified.
2. Either operation message monitoring or timer monitoring set by the "event timer" command can be set for each applet.
3. If a relevant applet deletes this command while an action set by the "action" command is running, the action will be executed until the end, but actions that have not been executed will not be executed.
4. The output contents of message text in operation messages may change when the software version is changed. When the software version is changed, check whether monitoring conditions need to be changed.

event timer

Performs timer monitoring.

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

Syntax

To set information:

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

To delete information:

no event timer

Input mode

```
(config-applet)
```

Parameters

cron <string>

Specifies monitoring conditions for the cron timer.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   - <minute>

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

   - <hour>

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

   - <day>

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

   - <month>

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

   - <week>

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

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

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

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

   - Wildcard (*)

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

   - Comma (,)

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

- Slash (/)

  Monitors are performed at intervals of the number specified on the right of a slash.
- Hyphen (-)

  The range of values can be specified by inserting a hyphen between numbers.

The following table shows examples of specifying <string>.

Table 13-1: Examples of specifying <string>

Specified value	Monitoring condition
"* * * * *"	Runs every minute.
"43 23 * * *"	Runs every day at 23:43.
"0 17 * * 1"	Runs every Monday at 17:00.
"0,10 17 * * 0,2,3"	Runs every Sunday, Tuesday, and Wednesday at 17:00 and 17:10.
"0-10 17 1 * *"	Runs every minute from 17:00 to 17:10 on the 1st day of every month.
"0 0 1,15 * 1"	Runs at 0:00 on the 1st and 15th days of every month and on Mondays.
"42 4 1 * *"	Runs at 4:42 on the 1st day of every month.
"0 21 * * 1-6"	Runs every Monday to Saturday at 21:00.
"0,10,20,30,40,50 * * * *"	Runs at 0, 10, 20, 30, 40, and 50 minutes past every hour.
"*/10 * * * *"	Runs every 10 minutes from 0 minute past every hour.
"* 1 * * *"	Runs every minute from 1:00 to 1:59 every day
"0 */1 * * *"	Runs at 0 minute past every hour
"0 * * * *"	Runs at 0 minute past every hour
"2 8-20/3 * * *"	Runs daily at 8:02, 11:02, 14:02, 17:02, and 20:02
"30 5 1,15 * *"	Runs at 5:30 on the 1st and 15th days of every month.

interval <seconds>

Specifies the monitoring time (in seconds) for the interval timer.

1. Default value when this parameter is omitted:

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

   Specify 1 to 4294967 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the event management program is restarted, the interval timer will generate events at intervals of the specified time (in seconds) starting from the time of the restart.
2. When the "disable" command or the "no disable" command is executed, or when the "priority" command is executed to set or change the applet execution priority, the interval timer will generate events at intervals of the specified time (in seconds) starting from the time of the command execution.
3. Either timer monitoring or operation message monitoring set by the "event sysmsg" command can be set for each applet.
4. If a relevant applet deletes this command while an action set by the "action" command is running, the action will be executed until the end, but actions that have not been executed will not be executed.

priority

Sets the priority of applet execution.

Syntax

To set or change information:

priority {high | normal | low | last}

To delete information:

no priority

Input mode

```
(config-applet)
```

Parameters

{high | normal | low | last}

Specifies the priority of applet execution.

high

Sets the priority of applet execution to high (The level of the priority is 6).

normal

Sets the priority of applet execution to medium (The level of the priority is 3).

low

Sets the priority of applet execution to low (The level of the priority is 1).

last

Sets the priority of applet execution to last. This priority notification is sent when there are no longer other priority notifications.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The priority of applet execution is set to medium.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A maximum of 1024 events for each execution priority are queued as waiting for action execution.

Therefore, if events occur frequently, events may be discarded, and actions may not be executed.

2. If you change the setting of this command for a relevant applet while an action set by the "action" command is running, the action will be executed until the end, but actions that have not been executed will not be executed.

resident-script

Specifies startup information for a resident script.

Syntax

To set information:

resident-script <script id> python <file name> [<args>...]

To delete information:

no resident-script <script id>

Input mode

```
(config)
```

Parameters

<script id>

Specifies a script ID that identifies a resident script.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4

python <file name>

Specifies a Python script to be started.

<file name>

Specifies the file name of the Python script.

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a string of no more than 99 characters including the extension (either ".py", ".pyc", or ".pyo").

   Characters that can be used are alphanumeric characters, dots (.), hyphens (-), underscores (_), tildes (~), and hats (^).

<args>...

Specifies command line arguments to be given at the Python script startup.

1. Default value when this parameter is omitted:

   None

2. Range of values:

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

   Specifiable characters are alphanumeric characters and special characters. If you specify multiple <args>, specify them separating each with a space. If you use special characters such as a

space in an <args>, enclose the string of the <args> in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

14 Ethernet

bandwidth

Assigns the bandwidth of a line. This setting is used for calculating the line usage rate on a network monitoring device.

Syntax

To set or change information:

bandwidth <kbit/s>

To delete information:

no bandwidth

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<kbit/s>

Assigns the line bandwidth in kbit/s.

This setting is used for the ifSpeed/ifHighSpeed/axsIfStatsHighSpeed (SNMP MIB) value of the applicable port, and has no impact on communication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10000000

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

Default behavior

The line speed of the applicable port becomes the bandwidth.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

description

Sets supplementary information. This command can be used as a comment about the port. Note that when this command is set, information can be checked by using the "show interfaces" operation command or ifDescr (SNMP MIB).

Syntax

To set or change information:

description <string>

To delete information:

no description

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<string>

Sets supplementary information for an Ethernet interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

null is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

duplex (gigabitethernet)

Sets the duplex mode for the following Ethernet interfaces:

- 10BASE-T/100BASE-TX/1000BASE-T
- 100BASE-TX/1000BASE-T/2.5GBASE-T
- SFP ports used for 1000BASE-T or 1000BASE-X

Syntax

To set or change information:

duplex { half | full | auto }

To delete information:

no duplex

Input mode

```
(config-if)
```

Ethernet interface

Parameters

{ half | full | auto }

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

The table below shows the combinations of line types and specifiable parameters. auto is set if a non-specifiable parameter for any line speed.

Table 14-1: Specifiable parameters

Line type	Specifiable parameters
1000BASE-T	auto (when speed auto/auto 1000 is specified)
10BASE-T/100BASE-TX/ 1000BASE-T	auto (when speed auto/auto 10/auto 100/auto 1000/auto 10 100/auto 10 100 1000 is specified) half (when speed 10/speed 100 is specified) full (when speed 10/speed 100 is specified)
100BASE-TX/1000BASE-T/ 2.5GBASE-T	auto (when speed auto/auto 100/auto 1000/auto 2500/auto 100 1000/auto 100 1000 2500/auto 1000 2500 is specified) half (when speed 100 is specified) full (when speed 100 is specified)
1000BASE-X	auto (when speed auto/auto 1000 is specified) full (when speed 1000 is specified)

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:

   None

Default behavior

auto is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied when the command is set.

Notes

1. For 1000BASE-X, if auto-negotiation is not used, you must set speed to 1000 and duplex to full. If the auto or auto 1000 parameter is specified in the "speed" command, full is set for duplex as a result of the auto-negotiation.
2. For 1000BASE-T and 2.5GBASE-T, the setting of duplex changes to auto, and full duplex is supported as a result of auto-negotiation.
3. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.

duplex (tengigabitethernet)

Sets the duplex mode for the following Ethernet interfaces:

- SFP+/SFP shared ports used for 1000BASE-T or 1000BASE-X

Syntax

To set or change information:

duplex { auto | full }

To delete information:

no duplex

Input mode

(config-if)

Ethernet interface

Parameters

{ auto | full }

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

auto

Determines the duplex mode by auto-negotiation.

full

Sets the port to full duplex (fixed) mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

auto is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied when the command is set.

Notes

1. When 10GBASE-R is used, the duplex and speed settings become disabled.
2. For 1000BASE-X, if auto-negotiation is not used, you must set speed to 1000 and duplex to full. If the auto or auto 1000 parameter is specified in the "speed" command, full is set for duplex as a result of the

auto-negotiation.

3. For 1000BASE-T, the setting of duplex changes to auto, and full duplex is supported as a result of auto-negotiation.
4. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.

flowcontrol

Sets flow control.

Syntax

To set or change information:

flowcontrol send {desired | on | off} [loose]

flowcontrol receive {desired | on | off}

To delete information:

no flowcontrol send

no flowcontrol receive

Input mode

```
(config-if)
```

Ethernet interface

Parameters

send {desired | on | off}

Specifies the behavior for sending flow-control pause packets. Specify the same settings as those for the behavior for receiving flow-control pause packets at the destination.

desired

If fixed mode is specified, pause packets are sent. If the auto-negotiation function is specified, whether pause packets are sent is determined through communication with the connected device.

on

Pause packets are sent.

off

Pause packets are not sent.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

loose

Loose flow control mode is set.

In loose mode, the pause-packet sending interval is longer than the transmission suppression time.

1. Default value when this parameter is omitted:

   Loose mode is not set.

2. Range of values:

   None

receive {desired | on | off}

Sets the behavior for receiving flow-control pause packets. Specify the same settings as those for the behavior for sending flow-control pause packets at the destination.

desired

If fixed mode is set, pause packets are received. If the auto-negotiation function is specified, whether pause packets are received is determined through communication with the connected device.

on

Pause packets are received.

off

Pause packets are not received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Behavior varies depending on the line type.

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

  The receive behavior is off but the send behavior is desired.

- For 100BASE-TX/1000BASE-T/2.5GBASE-T:

  The receive behavior is off but the send behavior is desired.

- For 1000BASE-X:

  The receive behavior is off but the send behavior is desired.

- For 10GBASE-R:

  The receive behavior is on but the send behavior is off.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When using the following ports with auto-negotiation, if you specify a combination other than "off" for the <receive> parameter and "off" for the <send> parameter, or if you omit the command, the receiving behavior will be "desired" and the sending behavior will be "on".

   Table 14-2: List of target ports

Model	Port number
AX2340S-24T4X	Ports 25-30
AX2340S-24TH4X	Ports 25-30
AX2340S-48T4X	Ports 53-54

Model	Port number
AX2340S-24P4X	Ports 25-30
AX2340S-24PH4X	Ports 25-30
AX2340S-48P4X	Ports 53-54
AX2340S-16P8MP2X	Ports 25-26

frame-error-notice

Sets the condition for sending a notification when a frame reception error or a frame sending error occurs. A frame reception error or a frame sending error indicates that a frame is discarded due to a failure in receiving or sending a frame, which is caused by a minor error. The cause of the failure is collected as statistics. If the number of error occurrences or the error occurrence rate over 30 seconds exceeds the value set by using this command, the error occurrences are reported. The settings of this command are applied to all ports of the Switch, and the sending side and the receiving side have the same settings.

If this configuration is not set, the error occurrences are reported when 15 or more errors occur in a 30-second interval.

The following table shows the list of error items that correspond to frame reception and frame sending errors.

Table 14-3: List of error items

No.	Error items	
	Receiving	Sending
1	• CRC errors • Fragments • Jabber • Symbol errors • Short frames • Long frames • Overrun	• Late collision • Excessive collisions • Underrun

If an error occurrence is reported, a log entry is displayed and a private SNMP notification is sent.

Syntax

To set or change information:

frame-error-notice [error-frames <frames>] [error-rate <rate>] [{ one-time-display | everytime-display | off }]

Note: At least one parameter must be specified.

To delete information:

no frame-error-notice

Input mode

```
(config)
```

Parameters

error-frames <frames>

Sets, as the error notification condition, the threshold for the number of error occurrences (number of error frames).

1. Default value when this parameter is omitted:

   15

2. Range of values:

   1 to 446400000

error-rate <rate>

Specifies, as the error notification condition, the threshold for the error occurrence rate as a percentage (%). The error occurrence rate is calculated as the rate of the number of error frames against the total number of frames. The fractional portion of the rate is truncated, and then it is compared with the set value. Note that if this parameter is omitted, the error occurrence rate is not regarded as a notification condition.

1. Default value when this parameter is omitted:

   The error occurrence rate is not regarded as a notification condition.

2. Range of values:

   1 to 100

The notification condition varies depending on whether the error-frames parameter and/or the error-rate parameter are set. The following table shows the error notification conditions depending on whether each parameter is set.

Table 14-4: List of error notification conditions

No.	Parameter		Receiving/ sending	Error notification condition
	error-frames	error-rate		
1	Omitted	Omitted	Receiving	The number of reception error frames is 15 or more.
2			Sending	The number of sending error frames is 15 or more.
3		Set	Receiving	The rate of reception error frames against the total number of reception frames is equal to or greater than the value set for <rate>. This setting does not regard the number of error occurrences as a notification condition.
4			Sending	The rate of sending error frames against the total number of sending frames is equal to or greater than the value set for <rate>. This setting does not regard the number of error occurrences as a notification condition.
5	Set	Omitted	Receiving	The number of reception error frames is equal to or greater than the value set for <frames>. This setting does not regard the error occurrence rate as a notification condition.
6			Sending	The number of sending error frames is equal to or greater than the value set for <frames>. This setting does not regard the error occurrence rate as a notification condition.
7		Set	Receiving	The number of reception error frames is equal to or greater than the value set for <frames>, and the rate of reception error frames against the total number of reception frames is equal to or greater than the value set for <rate>.
8			Sending	The number of sending error frames is equal to or greater than the value set for <frames>, and the rate of sending error frames against the total number of sending frames is equal to or greater than the value set for <rate>.

{ everytime-display | one-time-display | off }

Specifies whether to display a log entry when an error occurrence is reported. If a large number of errors occur continuously, this setting can prevent the log file from being filled with this log entry. Note that this parameter has no impact on private SNMP notifications. Use the "snmp-server host" command to specify whether to send a private SNMP notification. For details, see "snmp-server host" command.

everytime-display

Displays a log entry every time an error occurrence is reported.

one-time-display

Displays a log entry only when an error occurrence is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error occurrence after the restart is reported.

off

No log entries are displayed.

1. Default value when this parameter is omitted:

   one-time-display

2. Range of values:

   None

Default behavior

When 15 or more errors occur in a 30-second time interval, the error occurrences are reported. Displays a log entry only when an error occurrence is reported for the first time. No log entries are displayed for subsequent errors. Note, however, that if the applicable port is restarted, a log entry is displayed when the first error occurrence after the restart is reported.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you use this command to set the configuration, you must specify at least one parameter.
2. Entering this command disables the settings specified until then. If you want to inherit the old settings, use this command to specify the applicable parameter again.

interface gigabitethernet

Set the following items related to the Ethernet interface. Entering this command switches to config-if mode, in which information about the relevant port can be set.

- 10BASE-T/100BASE-TX/1000BASE-T port
- 100BASE-TX/1000BASE-T/2.5GBASE-T port
- SFP port

Syntax

To set information:

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

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

None

interface tengigabitethernet

Set the following items related to the Ethernet interface. Entering this command switches to config-if mode, in which information about the relevant port can be set.

- SFP+/SFP shared port

Syntax

To set information:

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

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

None

Notes

1. 10GBASE-R can be used only on models that support 10G uplink with an optional license and when the 10G uplink license is set.

link debounce

Sets the link-down detection time after a link failure is detected until the actual link-down occurs. When a large value is set, temporary link-downs will not be detected, thereby preventing instability of the link.

Syntax

To set or change information:

link debounce [time <milli seconds>]

To delete information:

no link debounce

Input mode

`(config-if)`

Ethernet interface

Parameters

time <milli seconds>

Sets the debounce timer value in milliseconds.

1. Default value when this parameter is omitted:

   3000 milliseconds

2. Range of values:

   Multiples of 100 from 0 to 10000

Default behavior

The value is set to 2000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the link is stable even when a link-down detection timer is not set, you do not need to set one.
2. If a value smaller than the default value (2000 milliseconds) is set for 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T/10GBASE-CU, the link might become unstable.

link up-debounce

Sets the link-up detection time after a link failure is detected until the actual link-up occurs. When a large value is set, a temporary link-up will not be detected, thereby preventing instability of the network status.

Syntax

To set or change information:

link up-debounce time <milli seconds>

To delete information:

no link up-debounce

Input mode

```
(config-if)
```

Ethernet interface

Parameters

time <milli seconds>

Sets the debounce timer value when a link-up state occurs, in milliseconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Multiples of 100 from 0 to 10000

Default behavior

When the line speed is fixed, the value is set to 1000 milliseconds. When the line speed is set to auto-negotiation, the value is set to 0 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The larger the value you set for the link-up detection timer, the more time it takes until communication is restored after a link failure has been corrected. If you want this time to be short, do not set a link-up detection timer.
2. If you set a value smaller than the default value, the link might become unstable.

mdix auto

Sets the AUTO-MDI/MDI-X function of the port to be used. When no mdix auto is specified, the AUTO-MDI/MDI-X function is disabled and the port is fixed to MDI-X.

Syntax

To set information:

no mdix auto

To delete information:

mdix auto

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is enabled during auto-negotiation.
2. For 1000BASE-X, this command is disabled.
3. For 10GBASE-R, this command is disabled.

mtu

Sets the MTU for ports. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

mtu <length>

To delete information:

no mtu

Input mode

(config-if)

Ethernet interface

Parameters

<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 on the frame format, see "Configuration Guide Vol. 1, 20.2.2 Frame format".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Multiples of 2 from 1500 to 9216

Default behavior

The following initial values are set.

Table 14-5: Initial MTU values for ports

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

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the MTU of the applicable port and the length of frames that can be sent or

received (the maximum length of frames in Ethernet V2 format#, excluding the FCS).

#: For details on the frame format, see "Configuration Guide Vol. 1, 20.2.2 Frame format".

Table 14-6: MTU and the length of frames that can be sent or received

Line type	mtu setting	system mtu Method	Length of frames that can be sent or received (octets)	Port MTU (octets)
10BASE-T (full duplex/half duplex), 100BASE-TX (half duplex)	Not related	Not related	Tagged 1518 Untagged 1518	1500
Other	Set	Not related	Tagged M1#1+18 Untagged M1#1+18	M1#1
	Not set	Set	Tagged M2#2+18 Untagged M2#2+18	M2#2
		Not set	Tagged 1518 Untagged 1518	1500

#1: The value set by using the "mtu" command of interface

#2: The value set by using the "system mtu" command

2. The MTU for a VLAN interface varies depending on the port MTU and the IP MTU setting.

Table 14-7: MTU for a VLAN interface

MTU setting	IP MTU setting	MTU of a VLAN interface (in octets)
Omitted	Omitted	1500
	Set	min (1500, L2#1)
Set	Omitted	L1#2
	Set	min (L1#2, L2#1)

#1: IP MTU value

#2: Port MTU value (if values differ among ports, the minimum value is used.)

3. For two row VLAN tags in VLAN tunneling, the frame length will be "IP packet length + 22 octets". If an IP packet of 1500 octets is send/received on a port with two-row VLAN tags, set a value equal to or larger than 1504 for mtu.

power inline

Sets the port priority. Setting the power priority for each port ensures that power is supplied to the appropriate ports.

Syntax

To set or change information:

power inline {critical | high | low | never}

To delete information:

no power inline

Input mode

```
(config-if)
```

Ethernet interface

Parameters

{critical | high | low | never}

Set the power supply priority for each port.

critical

Power is allocated to the most important port. Set this value for a port for which power must always be supplied.

high

Set the power supply priority to "High". If power becomes insufficient, the supply of power to ports with this specification stops only after power to ports with the low setting has stopped.

low

Set the power supply priority to "Low". If power becomes insufficient, the supply of power to ports with this specification stops before the supply of power to ports with the high setting.

never

Disables the PoE function of ports. When power is supplied, power is no longer supplied and the PoE function is disabled. If a connected device is a powered device, power is not supplied.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

"high" 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 remote device is power sourcing equipment, set "never" to disable the PoE function of the line.

power inline allocation

Set the power allocation for each port.

Syntax

To set or change information:

power inline allocation {auto | autoclass | limit <threshold>}

To delete information:

no power inline allocation

Input mode

```
(config-if)
```

Ethernet interface

Parameters

{auto | autoclass | limit <threshold>}

The following table shows the specifiable parameters for each model.

Table 14-8: Specifiable parameters for each model

Model	Specifiable parameter
AX2340S-24P4X AX2340S-24PH4X AX2340S-48P4X	auto limit
AX2340S-16P8MP2X	auto autoclass
Other	This command cannot be set.

auto

It automatically detects the powered device and classifies the power class, and sets the power amount allocation for the target port on a Class basis.

The following table shows the power classes and maximum output power to be allocated.

Table 14-9: Power classes and maximum output power to be allocated

Power class	Maximum output power
Class0	15.4 watts
Class1	4.0 watts
Class2	7.0 watts
Class3	15.4 watts
Class4	30.0 watts
Class5	45.0 watts
Class6	60.0 watts

autoclass

If a powered device supports the Autoclass function, this command measures the actual power of the powered device and allocates the measured power.

limit <threshold>

It automatically detects the powered device and classifies the power class, and manually set the power amount allocation for the target port.

Set the amount of power supplied to the port and the power consumption used for priority control in units of 200 milliwatts.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4000 to 30000 (milliwatts)

Default behavior

"auto" is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For settings by manual assignment, refer to the manual of the powered device and perform it at your own risk.
2. Set the maximum power consumption of the powered device to a value with some margin.
3. If you manually set a value smaller than the minimum power consumption required by the powered device, overload may be detected and power supply to the powered device may be stopped. To recover, execute the "activate power inline" operation command.
4. If you set, change, or delete the autoclass parameter and the applicable port is already powered, execute the "inactivate power inline" and "activate power inline" operation commands in that order. By stopping and restarting the power supply, the actual power allocation will change.

power inline delay

Set the PoE power supply start wait time for the Switch (the wait time from when the Switch is started or restarted until the Switch starts PoE power supply) and set the PoE port power supply start interval.

Syntax

To set or change information:

power inline delay system <seconds> port <seconds>

To delete information:

no power inline delay

Input mode

```
(config)
```

Parameters

system <seconds>

Set the PoE power supply start wait time for the Switch in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 3600 (seconds)

port <seconds>

Set the power supply start interval for the PoE port in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 60 (seconds)

Default behavior

The PoE power supply start wait time for the Switch works at 0 seconds. Also, the power supply start interval for the PoE port works at 0 seconds.

Impact on communication

None

When the change is applied

After changing the settings, save the configuration. The PoE power supply start wait time for the Switch is applied the next time the Switch starts or restarts. The power supply start interval for the PoE port will be applied from the next power supply distribution processing.

Notes

1. If you delete this command while the Switch is waiting for PoE power supply to start, the power supply

start wait state is canceled and PoE power supply starts.

2. This command is valid only on models that support PoE.

power inline priority-control disable

Prioritizes ports that are already powered.

Syntax

To set information:

power inline priority-control disable

To delete information:

no power inline priority-control disable

Input mode

```
(config)
```

Parameters

None

Default behavior

Port priority settings are enabled.

Impact on communication

None

When the change is applied

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

Notes

1. This command is valid only on models that support PoE.

shutdown

Places the port in the shutdown state.

Syntax

To set information:

shutdown

To delete information:

no shutdown

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

Communication using the relevant port becomes unavailable.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

speed (gigabitethernet)

Sets the speed of a port for the following Ethernet interfaces:

- 10BASE-T/100BASE-TX/1000BASE-T
- 100BASE-TX/1000BASE-T/2.5GBASE-T
- SFP ports used for 1000BASE-T or 1000BASE-X

Syntax

To set or change information:

speed { 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 2500 | 10 100 | 10 100 1000 | 100 1000 | 100 1000 2500 | 1000 2500} }

To delete information:

no speed

Input mode

```
(config-if)
```

Ethernet interface

Parameters

{ 10 | 100 | 1000 | auto | auto {10 | 100 | 1000 | 2500 | 10 100 | 10 100 1000 | 100 1000 | 100 1000 2500 | 1000 2500} }

Sets the line speed.

The table below shows the combinations of line types and specifiable parameters.

auto is set if a non-specifiable parameter for any line speed.

Table 14-10: Specifiable parameters

Line type	Specifiable parameters
1000BASE-T	auto auto 1000
10BASE-T/ 100BASE-TX/ 1000BASE-T	10 100 auto auto 10 auto 100 auto 1000 auto 10 100 auto 10 100 1000
100BASE-TX/ 1000BASE-T/ 2.5GBASE-T	100 auto auto 100 auto 1000 auto 2500

Line type	Specifiable parameters
	auto 100 1000 auto 100 1000 2500 auto 1000 2500
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 | 2500 | 10 100 | 10 100 1000 | 100 1000 | 100 1000 2500 | 1000 2500}

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

auto is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.
2. If auto-negotiation is not used for 10BASE-T, 100BASE-TX, or 1000BASE-T, you must set speed to 10 or 100, and set duplex to full or half.
3. If auto-negotiation is not used for 100BASE-TX, 1000BASE-T, or 2.5GBASE-T, you must set speed to 100, and set duplex to full or half.

4. For 1000BASE-X, if auto-negotiation is not used, you must set speed to 1000 and duplex to full.
5. For 100BASE-TX, 1000BASE-T, and 2.5GBASE-T, down-shifting to 100Mbit/s is not supported.

speed (tengigabitethernet)

Sets the speed of a port for the following Ethernet interfaces:

- SFP+/SFP shared ports used for 1000BASE-T or 1000BASE-X

Syntax

To set or change information:

speed {1000 | auto | auto 1000}

To delete information:

no speed

Input mode

(config-if)

Ethernet interface

Parameters

{1000 | auto | auto 1000}

Sets the line speed.

The table below shows the combinations of line types and specifiable parameters.

auto is set if a non-specifiable parameter for any line speed.

Table 14-11: Specifiable parameters

Line type	Specifiable parameters
1000BASE-T	auto auto 1000
1000BASE-X	1000 auto auto 1000

1000

Sets the line speed to 1000 Mbit/s.

auto

Sets the line speed to auto-negotiation.

auto 1000

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

auto is set.

Impact on communication

If this command is specified for a port in use, the port goes down and communication stops temporarily. The port then restarts.

When the change is applied

The change is applied when the command is set.

Notes

1. When 10GBASE-R is used, the duplex and speed settings become disabled.
2. If auto or a parameter containing auto is specified for speed or duplex, auto-negotiation is performed.
3. For 1000BASE-X, if auto-negotiation is not used, you must set speed to 1000 and duplex to full.

system flowcontrol off

Disables flow control for all ports on the device. This setting has priority over flow control settings for specific ports.

Syntax

To set information:

system flowcontrol off

To delete information:

no system flowcontrol off

Input mode

```
(config)
```

Parameters

None

Default behavior

The flow control setting specified for each port is used.

Impact on communication

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

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

None

system mtu

Sets the MTU of all ports. With this configuration, jumbo frames can be used to improve the throughput of data transfers. As a result, the usability of a network and devices connected to the network improves.

Syntax

To set or change information:

system mtu <length>

To delete information:

no system mtu

Input mode

```
(config)
```

Parameters

<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 on the frame format, see "Configuration Guide Vol. 1, 20.2.2 Frame format".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Multiples of 2 from 1500 to 9216 (octets)

Default behavior

The MTU of all ports is set to 1500.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The table below describes the port MTU and the length of a frame that can be sent or received (the maximum length of a frame in Ethernet V2 format#, excluding the FCS).

   #: For details on the frame format, see "Configuration Guide Vol. 1, 20.2.2 Frame format".

Table 14-12: MTU and the length of frames that can be sent or received

Line type	mtu setting	system mtu setting	Length of frames that can be sent or received (octets)	Port MTU (in octets)
10BASE-T (full duplex/half duplex), 100BASE-TX (half duplex)	Not related	Not related	Tagged 1518 Untagged 1518	1500
Other	Set	Not related	Tagged M1[#1]+18 Untagged M1[#1]+18	M1[#1]
	Not set	Set	Tagged M2[#2]+18 Untagged M2[#2]+18	M2[#2]
		Not set	Tagged 1518 Untagged 1518	1500

#1: The value set by using the "mtu" command of interface

#2: The value set by using the "system mtu" command

2. For two row VLAN tags in VLAN tunneling, the frame length will be "IP packet length + 22 octets". If an IP packet of 1500 octets is sent/received on a port with two-row VLAN tags, set system mtu so that the port mtu value is set to a value larger than 1504 or set a value larger than 1504 for mtu on the port.

15 Link Aggregation

channel-group lacp system-priority

Sets the LACP system priority of the applicable channel group for link aggregation.

Syntax

To set or change information:

channel-group lacp system-priority <priority>

To delete information:

no channel-group lacp system-priority

Input mode

`(config-if)`

Port channel interface

Parameters

<priority>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

The setting of the "lacp system-priority" command is used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down, and then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you set a function to restrict the number of detached ports (max-detach-port) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.
3. If the LACP system priority is changed, the status of all ports registered for the channel group changes to Blocking (communication interrupted).

channel-group max-active-port

Sets the maximum number of active ports that will be used for link aggregation in the applicable channel group.

Syntax

To set information:

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

To change information:

channel-group max-active-port <number>

channel-group max-active-port <number> no-link-down

To delete information:

no channel-group max-active-port

Input mode

```
(config-if)
```

Port channel interface

Parameters

<number>

Specifies the maximum number of ports that will be used for link aggregation in a channel group. If the number of ports that are actually used in a channel group exceeds the value specified by this command, only the specified maximum number of ports are used, and the standby link function is applied to the rest of the ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8

no-link-down

To use the standby link function in a link-not-down mode, specify this parameter. Otherwise, standby links switch to the link-down status. The criteria for selecting which links are standby links are as follows:

- Select ports that have been assigned lower priority by using the "lacp port-priority" command.
- If the priority is the same, select the port with the larger switch number, larger NIF number, and larger port number.

1. Default value when this parameter is omitted:

   Standby links switch to link-down status.

2. Range of values:

   None

Default behavior

The maximum number is 8.

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when static link aggregation is used.
2. If you specify the "max-active-port" command, match its settings to the settings of the "max-active-port" and "lacp port-priority" commands on the destination device.
3. Ports in standby link mode cannot be changed directly between the link-down and no-link-down statuses. To change the status, delete this parameter, and then set this parameter again. To change the number of ports in a link-not-down mode, you must specify the no-link-down parameter.
4. If this command is set and a port in link-down status is selected as a standby link, only the log entries that indicate detachment are displayed. Log entries indicating aggregation for the ports are not displayed.

channel-group max-detach-port

Limits the maximum number of detached ports in the applicable link aggregation channel group.

Syntax

To set or change information:

channel-group max-detach-port <number>

To delete information:

no channel-group max-detach-port

Input mode

`(config-if)`

Port channel interface

Parameters

<number>

Specifies the maximum number of ports that can be detached from a channel group used for link aggregation for reasons such as a link down. When 0 is specified, no ports can be detached. Therefore, if a link goes down, the whole channel group goes down.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 or 7

Default behavior

7 is set as the limit on the maximum number of detached ports.

Impact on communication

Channel groups might go down due to a function to restrict the number of detached ports.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you specify the "max-detach-port" command, match its settings to the settings of the destination device.
3. If 0 is entered for the "max-detach-port" command, the effect is the same as when 7 is entered for the "max-detach-port" command in on mode (this is the default when nothing is entered for max-detach-port).
4. If you set a function to restrict the number of detached ports (max-detach-port) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.

5. If you change the value for <number> to 0, all ports registered for the channel group change to Blocking (communication interrupted) while some ports registered in the channel group for the applicable link aggregation are degraded.

channel-group mode

Creates a channel group for link aggregation.

Syntax

To set information:

channel-group <channel group number> mode { on | { active | passive } }

To change information:

channel-group <channel group number> mode { active | passive }

To delete information:

no channel-group

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<channel group number>

Specifies the channel group number for link aggregation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

mode { on | { active | passive } }

Specifies the mode for link aggregation.

on

Static link aggregation is performed.

active

LACP-based link aggregation is performed, and LACPDUs are always sent irrespective of the remote device.

passive

LACP-based link aggregation is performed, but LACPDUs are sent only when an LACPDU from the remote device is received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

If this setting is specified for an active port, communication temporarily stops.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To change static link aggregation to LACP-based link aggregation, or vice versa, delete this command, change the mode, and then set the command again.
2. When channel-group mode is set, the port-channel setting of the specified channel group is automatically generated. If port-channel has already been set, no specific operation is required.
3. If the port-channel setting of the specified channel group number already exists when you set this command, you must either specify the same setting for the applicable interface and the port channel interface with the specified channel group number or else not set a common configuration command for the applicable interface. For details, see "Configuration Guide Vol. 1, 21.2.4 Configuring a port channel interface".
4. If you want to delete this command, do so after executing the "shutdown" command for the applicable interface.
5. Deleting this command does not delete the port-channel configuration (deleting all ports in a channel group does not delete the port-channel configuration). When deleting a channel group, you must delete the port-channel configuration manually.

channel-group periodic-timer

Specifies the interval for sending LACPDUs.

Syntax

To set or change information:

channel-group periodic-timer { long | short }

To delete information:

no channel-group periodic-timer

Input mode

```
(config-if)
```

Port channel interface

Parameters

{ long | short }

Specifies the sending interval at which the partner device sends LACPDUs to a Switch.

long: 30 seconds

short: one second

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

long (30 seconds) is set as the sending interval.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.

description

Sets supplementary information.

Syntax

To set or change information:

description <string>

To delete information:

no description

Input mode

```
(config-if)
```

Port channel interface

Parameters

<string>

Sets supplementary information for the applicable channel group used for link aggregation. Use this command to create and attach a note to the interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

NULL is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

interface port-channel

Sets an item related to a port channel interface. Entering this command switches to config-if mode, in which configuration commands can be set to specify the channel group number. A port channel interface is automatically generated when the "channel-group mode" command is set.

Syntax

To set information:

interface port-channel <channel group number>

To delete information:

no interface port-channel <channel group number>

Input mode

```
(config)
```

Parameters

<channel group number>

Specifies the channel group number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

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.

lacp port-priority

Sets the port priority.

Syntax

To set or change information:

lacp port-priority <priority>

To delete information:

no lacp port-priority

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<priority>

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

When on is specified for the "channel-group mode" command

This parameter is used with the "max-active-port" command to select the standby links.

When active or passive is set for the "channel-group mode" command

This parameter applies to port priority for the LACP protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

128 is set as the port priority.

Impact on communication

If you specify the port priority for an active port by setting channel-group mode to active or passive, communication is temporarily interrupted. If you specify port priority for active ports by setting channel-group mode to on, ports that are use might be changed by the standby link function, and communication might temporarily stop.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you specify the "max-active-port" command, match its settings to the settings of max-active-port for the destination device.
2. If you change <priority>, the status of the applicable port changes to Blocking (communication interrupted).

lacp system-priority

Sets the effective LACP system priority for a device.

Syntax

To set or change information:

lacp system-priority <priority>

To delete information:

no lacp system-priority

Input mode

```
(config)
```

Parameters

<priority>

Sets the LACP system priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

If the "channel-group lacp system-priority" command has been set, that setting is used. If the "channel-group lacp system-priority" command has not been set, 128 is used.

Impact on communication

If a priority is set for an active channel group, the channel group goes down, and then restarts.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is effective only when LACP-based link aggregation is used.
2. If you set a function to restrict the number of detached ports (max-detach-port) to connect a Switch to a device from other manufacturers, set a higher LACP system priority level for the Switch.
3. If the LACP system priority is changed, the status of all ports registered for the channel group changes to Blocking (communication interrupted).

shutdown

Always disables the applicable channel group for link aggregation, and stops communication.

Syntax

To set information:

shutdown

To delete information:

no shutdown

Input mode

`(config-if)`

Port channel interface

Parameters

None

Default behavior

None

Impact on communication

If a priority is specified for an active channel group, the channel group goes down.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

16 MAC Address Table

mac-address-table aging-time

Sets the aging conditions for MAC address table entries.

Syntax

To set or change information:

mac-address-table aging-time <seconds>

To delete information:

no mac-address-table aging-time

Input mode

```
(config)
```

Parameters

<seconds>

Sets the aging time in seconds. If 0 is specified, aging is not performed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0, 10 to 1000000 (seconds)

Default behavior

300 seconds is set as the aging time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A Switch checks for received frames each time the specified aging time elapses. Accordingly, at a maximum, twice the aging time might be required for the learned entries to be deleted.

mac-address-table learning

The "no mac-address-table learning" command suppresses dynamic MAC address learning for each VLAN. When MAC address learning is suppressed, frames with non-static entry among frames received in VLANs subject to learning suppression are flooded.

Syntax

To set information:

no mac-address-table learning vlan <vlan id list>

To change information:

no mac-address-table learning vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

To delete information:

mac-address-table learning vlan

Input mode

```
(config)
```

Parameters

vlan <vlan id list>

Specifies the list of VLANs for which MAC address learning is to be suppressed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

Modifies the specified VLAN list. add specifies VLANs to be added to the specified VLAN list, and remove specifies VLANs to be removed from the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

MAC address learning is not suppressed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If MAC address learning is suppressed, the MAC address table learned for target VLANs is deleted.

mac-address-table static

Sets static MAC address table information.

Syntax

To set or change information:

mac-address-table static <mac> vlan <vlan id> {interface <interface type> <interface number> | drop}

To delete information:

no mac-address-table static <mac> vlan <vlan id>

Input mode

```
(config)
```

Parameters

<mac>

Specifies a MAC address to be registered as a static entry.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to feff.ffff.ffff

   Note, however, that a multicast MAC address (address whose first-byte lowest bit is set to 1) cannot be set.

vlan <vlan id>

Specifies the VLAN ID of the VLAN for static entries.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

{interface <interface type> <interface number> | drop}

Specifies whether to forward or discard the frames that match the static entry.

interface <interface type> <interface number>

Specifies the output destination interface for static entries.

drop

Specifies that frames are discarded based on the static entry.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

   - Ethernet interface

- Port channel interface

Default behavior

No static entries are set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you set a static entry for the default VLAN (VLAN ID = 1), explicitly set "vlan 1" for the output destination interface.
2. If interface has been specified, a frame is output to the interface specified for frames matching the destination MAC address. In addition, if a frame is received from an interface other than the one specified for frames as matching the source MAC address, it is discarded.
3. If drop is specified, the frames matching the destination MAC address or source MAC address are discarded.
4. If a physical port in the channel group is specified as an output destination interface, communication might not be possible. Specify the port-channel parameter to set a channel group as the output destination for the static MAC address.
5. An authentication port for Layer 2 authentication cannot be set for the output destination interface.

17 VLAN

down-debounce

Sets the down-determination time of a VLAN interface when no more ports that can be used for relays exist in the VLAN.

Syntax

To set or change information:

down-debounce <seconds>

To delete information:

no down-debounce

Input mode

`(config-if)`

VLAN interface

Parameters

<seconds>

Sets the down-determination time (in seconds) of a VLAN interface when no more ports that can be used for relays exist in the VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 180

Default behavior

The VLAN interface goes down immediately when it is detected that there are no longer any ports that can be used for relaying the VLAN.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If there are no more ports that can be used for relaying the VLAN in the following situations, the VLAN interface goes down immediately regardless of any setting by this command:
   - When no more ports belong to the VLAN
   - When the VLAN status is disabled by the "state" command
2. If the setting value is changed during the down-determination time of a VLAN interface, the VLAN interface goes down after the changed setting value elapses since the time when the value was changed.
3. If the setting value is deleted during the down-determination time of a VLAN interface, the interface goes down when the value is deleted.

interface vlan

Sets a VLAN interface. Entering this command switches to config-if mode, in which the IP address or other settings can be set for the relevant VLAN interface.

Syntax

To set information:

interface vlan <vlan id>

To delete information:

no interface vlan <vlan id>

Input mode

```
(config)
```

Parameters

<vlan id>

Specifies a VLAN ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters". Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a VLAN ID which has not yet been set is specified for <vlan id>, a VLAN is created. Created VLANs are port VLANs. For a protocol VLAN or MAC VLAN, the VLAN must be created beforehand by using the "vlan" command.
2. If you set information for multiple VLAN interfaces, use the "interface range" command to set <vlan id list>. Note that an error will occur if you specify a VLAN ID which has not been set by using the "interface range" command, and a new VLAN will not be created.
3. Specifying no vlan for a VLAN that was created by the "interface vlan" command deletes the VLAN. Also, specifying the "no interface vlan" command for a VLAN that was created by the "vlan" command deletes the VLAN.

l2protocol-tunnel eap

Enables the EAPOL forwarding function. The function is set for a device.

Syntax

To set information:

l2protocol-tunnel eap

To delete information:

no l2protocol-tunnel eap

Input mode

```
(config)
```

Parameters

None

Default behavior

The EAPOL forwarding function is invalid.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

l2protocol-tunnel stp

Enables the BPDU forwarding function. The function is set for a device.

Syntax

To set information:

l2protocol-tunnel stp

To delete information:

no l2protocol-tunnel stp

Input mode

```
(config)
```

Parameters

None

Default behavior

The BPDU forwarding function is invalid.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

mac-address

Sets the MAC address used to identify a MAC VLAN.

Syntax

To set information:

mac-address <mac>

To delete information:

no mac-address <mac>

Input mode

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

Parameters

<mac>

Specifies the MAC address setting for a MAC VLAN. This command can be set only when the applicable VLAN is a MAC VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to feff.ffff.ffff

   The lowest bit of the first byte (the multicast bit) must not be 1.

Default behavior

No MAC address is specified.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. MAC addresses that are already assigned to another VLAN cannot be set. Delete the address, and then set it again.
2. If you specify a dynamically-set MAC address used for IEEE 802.1X, Web authentication, or MAC-based authentication, settings for those functions become invalid and settings for this command are enabled.
3. The maximum number of MAC addresses that can be set for a device is 64.

name

Sets a VLAN name.

Syntax

To set or change information:

name <string>

To delete information:

no name

Input mode

```
(config-vlan)
```

Parameters

<string>

Sets a VLAN name. This parameter cannot be set if <vlan id list> has been specified by using the "vlan" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The initial value is "VLANxxxx". Note that "xxxx" is a four-digit numeric string, including any leading zeros, that indicates a VLAN ID.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

protocol

Sets the protocol for identifying VLANs in protocol VLANs.

Syntax

To set information:

protocol <protocol name>

To delete information:

no protocol <protocol name>

Input mode

```
(config-vlan)
```

Parameters

<protocol name>

Specifies the name of the protocol in a protocol VLAN. This command can be set only when the applicable VLAN is a protocol VLAN. If you want to use multiple protocols in a single VLAN, specify this command as many times as the number of protocol names.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Protocol name set by the "vlan-protocol" command

Default behavior

No protocol is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To use a protocol VLAN with an IPv4 address or IPv6 address set, you must use this command to specify the applicable protocol.

state

Sets the VLAN status.

Syntax

To set or change information:

state {suspend | active}

To delete information:

no state

Input mode

```
(config-vlan)
```

Parameters

{suspend | active}

suspend

Disables the VLAN status and stops the sending and receiving of all frames on the VLAN.

active

Sets the VLAN status to enable and starts the sending and receiving of all frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The VLAN status is enable.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

switchport access

Sets access port information. The information you set is also applied to access VLANs of tunneling ports.

Syntax

To set or change information:

switchport access vlan <vlan id>

To delete information:

no switchport access vlan

Input mode

(config-if)

Ethernet interface, port channel interface

Parameters

vlan <vlan id>

Sets an interface to the access port for the specified VLAN (access VLAN). The access VLAN for the tunneling port is also the specified VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

Default behavior

In non-VLAN tunneling mode, the access port for the default VLAN (VLAN ID = 1) is used. The default behavior in VLAN tunneling mode is for switch ports to not belong to any VLAN and for communication with VLANs to be disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. In non-VLAN tunneling mode, if an untagged frame or an access VLAN tagged frame is received, the frame is handled by the access VLAN. If a tagged frame of a VLAN other than an access VLAN is received, the frame is discarded.
2. In VLAN tunneling mode, frames are handled by access VLANs irrespective of whether they have a VLAN tag.

switchport dot1q ethertype

Sets the TPID (Tag Protocol IDentifier) value that identifies VLAN frames on a port. This command is set when you connect to a network in which a non-standard TPID value is used.

Syntax

To set or change information:

switchport dot1q ethertype <hex>

To delete information:

no switchport dot1q ethertype

Input mode

`(config-if)`

Ethernet interface

Parameters

<hex>

Sets the TPID value of a VLAN tag which is assigned by a Switch. This command sets the default value for ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Four-digit hexadecimal

Default behavior

When the "vlan-dot1q-ethertype" command is set, the setting value for the command is regarded as the TPID value. When the "vlan-dot1q-ethertype" command is not set, 0x8100 is regarded as the TPID value.

Impact on communication

When configuring or deleting, frames may be discarded or the same frame may be sent from multiple ports until the port allocation for the frame transmission of the link aggregation of the Switch is applied.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For ports specified by using this command, the value specified for vlan-dot1q-ethertype is not applied.
2. A maximum of four TPID values can be specified per device.

switchport isolation

Configures the inter-port forwarding block function.

Syntax

To set information:

switchport isolation interface <interface id list>

To change information:

switchport isolation interface {<interface id list> | add <interface id list> | remove <interface id list>}

To delete information:

no switchport isolation

Input mode

```
(config-if)
```

Ethernet interface

Parameters

interface <interface id list>

Specifies a list of physical ports from which forwarding is to be blocked. Forwarding from the specified ports to the interface is suppressed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

interface add <interface id list>

Adds ports forwarding from which is to be isolated to the list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

interface remove <interface id list>

Removes ports forwarding from which is isolated from the list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

Forwarding between ports is not isolated.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The function for suppressing inter-port forwarding is entered from the line specified by interface of the "switchport isolation" command, and discards frames output from the port on which the command is set. To suppress forwarding on both ends, set the command on both lines.
2. If you use interface range to configure information for multiple interfaces, only one physical port can be specified.
   If you want to specify a list of ports for which to suppress forwarding, set the information for a single interface.

switchport mac

Sets MAC VLAN port information.

Syntax

To set information:

switchport mac vlan <vlan id list>

switchport mac native vlan <vlan id>

switchport mac dot1q vlan <vlan id list>

To change information:

switchport mac {vlan <vlan id list> | vlan add <vlan id list> | vlan remove <vlan id list> | native vlan <vlan id> | dot1q vlan <vlan id list> | dot1q vlan add <vlan id list> | dot1q vlan remove <vlan id list>}

To delete information:

no switchport mac vlan

no switchport mac native vlan

no switchport mac dot1q vlan

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

vlan <vlan id list>

Specifies the list of valid MAC VLANs that applies to a switch port. When this value is changed, a list of the currently-valid MAC VLANs replaces the specified list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

native vlan <vlan id>

Sets the VLAN that can receive frames with unregistered source MAC addresses. Frames can also be sent from the specified VLAN. Specifiable VLANs are port VLANs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

dot1q vlan <vlan id list>

Sends the frames of the VLANs in the VLAN list set by using this parameter in the form of tagged frames. It is also possible to forward the tagged frames set by using this parameter. If a tagged frame is received by another VLAN, the frame is discarded.

VLANs configured by using the vlan parameter cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

vlan add <vlan id list>

Adds the currently-valid MAC VLANs for this port to the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

vlan remove <vlan id list>

Removes the valid MAC VLANs for this port from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

dot1q vlan add <vlan id list>

Adds a VLAN able to forward tagged frames on the port to the VLAN list. VLANs configured by using the vlan parameter cannot be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

dot1q vlan remove <vlan id list>

Removes a VLAN able to forward tagged frames on the port from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

None. If a MAC VLAN port has been set by using the "switchport mode" command with the mac-vlan parameter, and the "switchport mac" command has not been set, only the default VLAN is set. However, a MAC VLAN specified as a post-authentication VLAN by linking with the authentication function is available for communication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The MAC VLAN specified as a post-authentication VLAN by the authentication function is available for communication only when a valid MAC VLAN has not been set.
2. If valid MAC VLANs have been set, a MAC VLAN specified as a post-authentication VLAN by the authentication function is available for communication only when it matches a MAC VLAN that has been set. Therefore, if an authenticated terminal exists when a valid MAC VLAN has not been set, setting a valid MAC VLAN cancels the authentication of the terminal.

switchport mode

Sets Layer 2 interface attributes.

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)
```

Ethernet interface, port channel interface

Parameters

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

Sets Layer 2 interface attributes.

access

Sets the applicable interface to access mode. When non-VLAN tunneling is used, untagged frames are sent or received in access mode. When VLAN tunneling is used, frames are sent or received in an access VLAN irrespective of whether the frames have a VLAN tag. Ports in access mode can be used only in a single VLAN.

trunk

Sets an interface to trunking mode. In trunking mode, untagged frames and tagged frames are sent and received.

protocol-vlan

Sets an interface to protocol VLAN mode. In protocol VLAN mode, untagged frames are sent and received. When a frame is received, the VLAN is determined by the protocol type of the frame. Tagged frames are discarded.

mac-vlan

Sets an interface to MAC VLAN mode. In MAC VLAN mode, untagged frames are sent and received. When a frame is received, the corresponding VLAN is determined from the source MAC address of the frame. Tagged frames are discarded. Note, however, that if the dot1q vlan parameter is set for the "switchport mac" command, tagged frames are sent and received.

If the vlan parameter is not set in the "switchport mac" command, a MAC VLAN specified as a post-authentication VLAN by linking with the authentication function is available for communication.

dot1q-tunnel

Sets an interface to tunneling mode. In tunneling mode, frames are sent and received on an access VLAN irrespective of whether the frames have a VLAN tag.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

access (access mode) is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If an interface is set to trunking mode, set allowed vlan by using the "switchport trunk" command. If an interface is set to trunking mode and allowed vlan is not set, all frames on the applicable port are discarded.
2. If an interface is set to protocol VLAN mode, use the "switchport protocol" command to set a protocol VLAN. If protocol VLAN is not set, the behavior of the applicable port is the same as in access mode.
3. If an interface is set to tunneling mode, use the "switchport access" command to set an access VLAN. Ports in tunneling mode are not automatically added to the default VLAN. Even when the default VLAN is used as the access VLAN, use the "switchport access" command to explicitly enable the access VLAN. If an access VLAN is not set, communication is not possible on tunneling ports.
4. If there are any ports on the device that are configured for tunneling mode, the entire device enters VLAN tunneling mode. As a result, the behavior of the ports in access mode is the same as in tunneling mode.

switchport protocol

Sets protocol VLAN port information.

Syntax

To set information:

switchport protocol vlan <vlan id list>

switchport protocol native vlan <vlan id>

To change information:

switchport protocol {vlan <vlan id list> | vlan add <vlan id list> | vlan remove <vlan id list> | native vlan <vlan id>}

To delete information:

no switchport protocol vlan

no switchport protocol native vlan

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

vlan <vlan id list>

Sets the currently-valid protocol VLANs on the port. When this parameter is changed, the currently-valid protocol VLAN list replaces the specified list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

native vlan <vlan id>

Sets a VLAN that sends and receives frames of a protocol that does not match the configuration. Specifiable VLANs are port VLANs.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

vlan add <vlan id list>

Adds a currently-valid protocol VLAN on the port to the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

values for parameters".

vlan remove <vlan id list>

Removes a currently-valid protocol VLAN on the port from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

None. If a protocol VLAN port has been set by using the "switchport mode protocol" command and the "switchport protocol" command is omitted, the default VLAN is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If no currently-valid protocol VLANs are set, the behavior of the port is the same as an access port.
2. If multiple protocol VLANs are set for a protocol VLAN port, be careful that you do not duplicate the protocols for the protocol VLAN.

switchport trunk

Sets trunk port information.

Syntax

To set information:

switchport trunk allowed vlan <vlan id list>

switchport trunk native vlan <vlan id>

To change information:

switchport trunk native vlan <vlan id>

switchport trunk allowed vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

To delete information:

no switchport trunk allowed vlan

no switchport trunk native vlan

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

native vlan <vlan id>

Sets the native VLAN (VLAN that sends and receives untagged frames). Specifiable VLANs are port VLANs. If the native VLAN is not set explicitly, the default VLAN becomes the native VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

allowed vlan <vlan id list>

Sets the VLANs that use a trunk port for sending and receiving frames.

The frames of VLANs that have not been specified are discarded.

To send and receive untagged frames, you must specify the native VLAN. If you do not set the native VLAN to allowed vlan, untagged frames are discarded.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

add <vlan id list>

Adds a VLAN to the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

remove <vlan id list>

Removes a VLAN from the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

Default behavior

None. If trunking mode has been set by using the "switchport mode trunk" command and the command is omitted, communication is not possible.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If an interface is set to trunking mode, you must set allowed vlan. If allowed vlan is not set, no frames will be sent from or received at the applicable interface.

switchport validation

Configure to discard specific frames.

Syntax

To set or change information:

switchport validation [vlan-tag] [ethernet-llc]

Note: At least one parameter must be specified.

To delete information:

no switchport validation

Input mode

```
(config-if)
```

Ethernet interface

Parameters

vlan-tag

Discard the following frames.

- The VLAN tag assigned to the frame is 2 or more levels, and the VLAN ID of the 1st level tag is '0'
- The VLAN tag assigned to the frame is 2 or more levels, and the VLAN ID of the 2nd level tag is '0'

1. Default value when this parameter is omitted:

   Not subject to discard

2. Range of values:

   None

ethernet-llc

Discard the following frames.

- 802.3 LLC/SNAP format frame, LENGTH is 1501 to 1535

1. Default value when this parameter is omitted:

   Not subject to discard

2. Range of values:

   None

Default behavior

Does not discard frames.

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 for a port belonging to a channel group, make the setting for all ports belonging to the corresponding channel group.
2. Setting to the tunneling port is not supported.

switchport vlan mapping

Sets tag translation information entries.

Syntax

To set or change information:

switchport vlan mapping <vlan tag> <vlan id>

To delete information:

no switchport vlan mapping <vlan tag> <vlan id>

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<vlan tag>

Specifies the VLAN tag value used in a LAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4094

<vlan id>

Specifies the VLAN ID of a VLAN that handles frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

Default behavior

Tag translation is not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To enable tag translation, you must specify switchport vlan mapping enable.
2. Tag translation is enabled only when the applicable port is in trunking mode.

3. Do not specify the VLAN ID of the native VLAN for a VLAN tag or the VLAN ID.
4. Only VLAN tags for which switchport vlan mapping is set can be sent and received on the ports for which tag translation is enabled. For the ports that use tag translation, set the "switchport vlan mapping" command even if the VLAN tags to be sent or received match the VLAN IDs.
5. In a session using the 802.1Q tagging function of port mirroring, when setting tag translation for the port specified as a mirror port, the VLAN tag to be set with this command must be a value different from VLAN IDs used by the 802.1Q tagging function.
6. Cannot use the same VLAN tag with a different VLAN ID or different VLAN tag with the same VLAN ID for all tag translation information entries for the Switch.

switchport vlan mapping enable

Enables tag translation.

Syntax

To set information:

switchport vlan mapping enable

To delete information:

no switchport vlan mapping enable

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

Tag translation is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To enable tag translation, you must specify switchport vlan mapping.
2. Tag translation is enabled only when the applicable port is in trunking mode.
3. Only VLAN tags for which switchport vlan mapping is set can be sent and received on the ports for which tag translation is enabled. For the ports that use tag translation, set the "switchport vlan mapping" command even if the VLAN tags to be sent or received match the VLAN IDs.

up-debounce

Sets the up-determination time for a VLAN interface after the VLAN interface goes down until another port in the VLAN comes up again as a port that can be used for communication.

Syntax

To set or change information:

up-debounce <seconds>

To delete information:

no up-debounce

Input mode

```
(config-if)
```

VLAN interface

Parameters

<seconds>

Sets the up-determination time (in seconds) for a VLAN interface when another port in the VLAN comes up as a port that can be used for communication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600

Default behavior

If a port in the VLAN comes up, and becomes available to restore communication, the VLAN interface comes up immediately.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. In the following situations, if a port in a VLAN comes up, and becomes available to restore communications, the VLAN interface comes up immediately, irrespective of the setting of this command:
   - When the device starts up
   - When the VLAN status is changed from disable to enable by using the "state" command
2. For a VLAN interface, if the setting value is changed during the up-determination time, the VLAN interface goes up after the changed setting value elapses since the time when the value was changed.
3. If the setting value is deleted during the up-determination time of a VLAN interface, the interface goes up when the value was deleted.

vlan

Sets VLAN-related items.

Syntax

To set information:

vlan <vlan id>

vlan <vlan id list>

vlan <vlan id> protocol-based

vlan <vlan id list> protocol-based

vlan <vlan id> mac-based

vlan <vlan id list> mac-based

To delete information:

no vlan <vlan id>

no vlan <vlan id list>

Input mode

```
(config)
```

Parameters

<vlan id>

Specifies a VLAN ID. When this command is entered, the mode switches to config-vlan mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters". Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

<vlan id list>

Specifies multiple VLAN IDs at one time. If you specify a VLAN ID for the first time, the applicable VLAN is newly created. When this command is entered, the mode switches to config-vlan mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters". Note, however, that the default VLAN (VLAN ID = 1) cannot be specified when information is deleted.

protocol-based

Specify this parameter for a protocol VLAN.

1. Default value when this parameter is omitted:

   The VLANs become port VLANs.

2. Note on using this parameter:

- To specify protocol VLANs, you must specify protocol-based.
- This parameter cannot be specified for any VLAN which has already been created as a port VLAN or a MAC VLAN.
- This parameter and the VLAN tunneling function cannot be used at the same time.

mac-based

Specifies this parameter for MAC VLANs.

1. Default value when this parameter is omitted:

   The VLANs become port VLANs.

2. Note on using this parameter:

   - When specifying MAC VLANs, you must specify mac-based.
   - This parameter cannot be specified for any VLAN which has already been created as a port VLAN or a protocol VLAN.
   - This parameter and the VLAN tunneling function cannot be used at the same time.

Default behavior

No VLANs are configured.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. There is always a default VLAN (VLAN ID = 1). The configuration items for the VLAN are different from those of other normal VLANs.
2. If you specify a list by using <vlan id list>, you can configure multiple VLANs at the same time. Note, however, that if a list is specified (for multi-command mode) some commands cannot be used. For details, see the following table.

   Table 17-1: Command availability in multi-command mode

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

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

3. The default VLAN setting (VLAN ID=1) always exists in the configuration file and cannot be deleted. The initial state of the default VLAN is for all ports to be available as access ports.
4. The table below explains parameter items that can be set for the default VLAN, and behavior specific to the default VLAN.

   vlan command:

   The following table applies to the "vlan" command.

Table 17-2: Handling default VLAN parameters

No.	Parameter	Whether specifiable by the user	Behavior specific to the default VLAN
1	<vlan id>	F (fixed value)	Set when the device starts up. Fixed at "1". Cannot be changed or deleted.
2	<vlan id list>	N	—
3	protocol-based	N	Port VLAN
4	mac-based	N	Port VLAN

Legend: F: Can be set as a fixed value; N: Cannot be set; —: Not applicable

config-vlan mode command:

The following table applies to the "config-vlan" mode command.

Table 17-3: Handling default VLAN parameters

No.	Command	Parameter	User setting availability	Default VLAN Unique behavior
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 create a VLAN, information can be set for the VLAN interface by using the "interface vlan" command. For VLANs created by using the "vlan" command, use the "no interface vlan" command to delete information. For a VLAN created by using the "interface vlan" command, use the "no vlan" command to delete information.

vlan-dot1q-ethertype

Sets the TPID for a VLAN tag.

Syntax

To set or change information:

vlan-dot1q-ethertype <hex>

To delete information:

no vlan-dot1q-ethertype

Input mode

```
(config)
```

Parameters

<hex>

Sets the TPID value of a VLAN tag which is assigned by a Switch. This command sets the default value of the entire device.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Four-digit hexadecimal

Default behavior

0x8100 is used as the TPID value. Note, however, that lines for which switchport dot1q ethertype is set, the setting value is used as the TPID value.

Impact on communication

When configuring or deleting, frames may be discarded or the same frame may be sent from multiple ports until the port allocation for the frame transmission of the link aggregation of the Switch is applied.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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>...] [llc <hex>...] [snap-ethertype <hex>...]

To delete information:

no vlan-protocol <protocol name>

Input mode

```
(config)
```

Parameters

<protocol name>

Sets the protocol name used for configuring the protocol VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A string with 14 or fewer characters

ethertype <hex>

Specifies the EtherType value for an Ethernet V2-format frame.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Four-digit hexadecimal

3. Note on using this parameter:

   EtherType values which have already been set by users cannot be specified.

llc <hex>

Specifies the LLC value (DSAP and SSAP) for 802.3-format frames.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Four-digit hexadecimal

3. Note on using this parameter:

   LLC values which have already been set by users cannot be specified.

snap-ethertype <hex>

Specifies the EtherType value for an 802.3-format frame.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   Four-digit hexadecimal

3. Note on using this parameter:

   EtherType values which have already been set by users cannot be specified.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. Note, however, that for protocols that have not been specified by the "protocol" command for the protocol VLAN, the change is applied when the protocol name is specified by the "protocol" command.

Notes

None

vlan-up-message

The "no vlan-up-message" command suppresses the sending of operation messages as well as linkUp and linkDown traps when the VLAN status is Up or Down.

Syntax

To set information:

no vlan-up-message

To delete information:

vlan-up-message

Input mode

```
(config)
```

Parameters

None

Default behavior

Sends operation messages as well as linkUp and linkDown traps when the VLAN status is Up or Down.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The ifLinkUpDownTrapEnable value of the ifMIB group for VLAN is not affected by the setting of this command.

18 Spanning Tree Protocols

instance

Sets VLANs belonging to Multiple Spanning Tree MST instances.

Syntax

To set or change information:

instance <mst instance id> vlans <vlan range>

To delete information:

no instance <mst instance id>

Input mode

```
(config-mst)
```

Parameters

<mst instance id>

Sets an MST instance ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

vlans <vlan range>

Sets VLANs belonging to MST instances. One VLAN ID can be set. You can perform a batch setup of multiple VLAN IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4094

3. Note on using this parameter:

   - All VLANs that do not belong to other MST instances participate in MST instance ID0.
   - To configure the same MST region, the MST instance ID and the VLAN ID set by this parameter, as well as the values of the name parameter and the revision parameter, must match within the MST region.

Default behavior

All VLANs belong to MST instance ID0.

Impact on communication

When the "spanning-tree mode" command is used to set mst, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The "show" command does not display information about MST instance ID0.

name

Sets a string to identify a Multiple Spanning Tree region.

Syntax

To set or change information:

name <name>

To delete information:

no name

Input mode

```
(config-mst)
```

Parameters

<name>

Sets the character string used to identify a region.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

3. Note on using this parameter:

   To configure the same MST region, the values for this parameter and the revision parameter, as well as those of the MST instance ID and the VLAN ID set by the vlans parameter, must match within the MST region.

Default behavior

name is set to NULL.

Impact on communication

When the "spanning-tree mode" command is used to set mst, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

revision

Sets a revision number to identify a Multiple Spanning Tree region.

Syntax

To set or change information:

revision <version>

To delete information:

no revision

Input mode

```
(config-mst)
```

Parameters

<version>

Sets the revision number to identify a region.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

3. Note on using this parameter:

   To configure the same MST region, the values for this parameter and the name parameter, as well as those of the MST instance ID and the VLAN ID set by the vlans parameter, must match within the MST region.

Default behavior

revision is set to 0.

Impact on communication

When the "spanning-tree mode" command is used to set mst, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree bpdufilter

Sets the BPDU filter function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

spanning-tree bpdufilter enable

To delete information:

no spanning-tree bpdufilter

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the BPDU guard function is disabled.

spanning-tree bpduguard

Sets the BPDU guard function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree) for which the PortFast function has been set.

Syntax

To set or change information:

spanning-tree bpduguard { enable | disable }

To delete information:

no spanning-tree bpduguard

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{ enable | disable }

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The setting of the "spanning-tree portfast bpduguard default" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree cost

Sets the path cost of the applicable port. This command is applied to all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree cost <cost>

To delete information:

no spanning-tree cost

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<cost>

Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   When short is set by the "spanning-tree pathcost method" command:

   1 to 65535

   When long is set by the "spanning-tree pathcost method" command:

   1 to 200000000

3. Note on using this parameter:

   Changing the path cost value might change the topology.

Default behavior

The method of applying the path cost is set by the "spanning-tree pathcost method" command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the "spanning-tree vlan cost" command, the "spanning-tree single cost" command, or the "spanning-tree mst cost" command is set, the value of the "spanning-tree cost" command is not applied.

2. When the "spanning-tree vlan pathcost method" command or the "spanning-tree single pathcost method" command is set, the value of the "spanning-tree cost" command is not applied.

spanning-tree disable

Stops operation of the Spanning Tree function for all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

spanning-tree disable

To delete information:

no spanning-tree disable

Input mode

```
(config)
```

Parameters

None

Default behavior

The Spanning Tree Protocols are enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree guard

Sets the guard function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree guard { loop | none | root }

To delete information:

no spanning-tree guard

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{ loop | none | root }

If loop is set, the loop guard function is applied to the applicable ports. The loop guard function does not work for Multiple Spanning Tree.

If none is set, the guard function of the applicable port is stopped.

If root is set, the root guard function is applied to the applicable ports.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The setting of the "spanning-tree loopguard default" command is used.

Impact on communication

When the loop guard function is set for a port or channel group that does not receive BPDU, even after one such port comes UP, communications of the port might remain disabled, or it might take time until communication is enabled.

When the change is applied

When settings for the "spanning-tree portfast default" command or the "spanning-tree portfast" command are deleted, if you change the configuration stored in memory without setting the "spanning-tree portfast default" command or the "spanning-tree portfast" command, the changes take effect immediately after the change.

Notes

1. If the "spanning-tree portfast default" command or the "spanning-tree portfast" command are set, the changes are not applied.

2. After the loop guard function is set, if a device starts, a port (including a port in a channel group) comes up, a Spanning Tree program is restarted, or the Spanning Tree type is changed, then the loop guard function blocks the port. The loop guard function is not cleared until a BPDU is received.
3. If loop guard function is set while a port is on line, the function is not enabled. Loop guard function, set while a port is on line, is enabled when a BPDU reception timeout occurs.

spanning-tree link-type

Sets the link type of the applicable port. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree). If you want to change the high-speed topology when rapid-pvst or mst is set by the "spanning-tree mode" command, and rapid-pvst is set by the "spanning-tree vlan mode" command, the connection between bridges must be a Point-to-Point connection. If you want to change the high-speed topology when rapid-stp is set by the "spanning-tree single mode" command, the connection between bridges must be a Point-to-Point connection.

Syntax

To set or change information:

spanning-tree link-type { point-to-point | shared }

To delete information:

no spanning-tree link-type

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{ point-to-point | shared }

If point-to-point is set, Point-to-Point connection is used for the link type. If shared is set, a shared connection is used for the link type.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

point-to-point is used for a full duplex port 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 function is enabled if point-to-point is set in STP compatibility mode. The automatic-restoration function does not work if shared is set in STP compatibility mode.

spanning-tree loopguard default

Sets the loop guard function that is used by default. This command is valid for ports of all Spanning Tree Protocols (PVST+ and Single Spanning Tree).

Syntax

To set information:

spanning-tree loopguard default

To delete information:

no spanning-tree loopguard default

Input mode

```
(config)
```

Parameters

None

Default behavior

If the "spanning-tree guard" command is set, that setting is used. If the "spanning-tree guard" command is not set, this command has no effect.

Impact on communication

When loop guard function is set for a port or channel group that does not receive BPDU, even after one such port comes UP, communications of the port might remain disabled, or it might take time until communication is enabled.

When the change is applied

When settings for the "spanning-tree portfast default" command or the "spanning-tree portfast" command are deleted, if you change the configuration stored in memory without setting the "spanning-tree portfast default" command or the "spanning-tree portfast" command, the changes take effect immediately after the change.

Notes

1. If the "spanning-tree portfast default" command or the "spanning-tree portfast" command are set, the changes are not applied.
2. After the loop guard function is set, if a device starts, a port (including a port in a channel group) comes up, a Spanning Tree program is restarted, or the Spanning Tree type is changed, then the loop guard function blocks the port. The loop guard function is not cleared until a BPDU is received.
3. If loop guard function is set while a port is on line, the function is not enabled. Loop guard function, set while a port is on line, is enabled when a BPDU reception timeout occurs.

spanning-tree mode

The following explains settings for the Spanning Tree running mode. This command applies to all Spanning Tree Protocols (PVST+ and Multiple Spanning Tree) other than Single Spanning Tree. If the "spanning-tree vlan mode" command is set in PVST+ running mode, the settings for that command are used.

Syntax

To set or change information:

spanning-tree mode { pvst | rapid-pvst | mst }

To delete information:

no spanning-tree mode

Input mode

```
(config)
```

Parameters

{ pvst | rapid-pvst | mst }

Sets the protocol to be used. If the protocol is changed while using Spanning Tree, the Spanning Tree Protocol is re-initialized. If pvst is set, PVST+ is applied to all Spanning Tree Protocols. If rapid-pvst is set, rapid PVST+ is applied to all Spanning Tree Protocols. If mst is set, this defines all Spanning Tree Protocols as belonging to Multiple Spanning Tree. For Single Spanning Tree, pvst or rapid-pvst must be set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The configuration is explicitly set to spanning-tree mode pvst.

Impact on communication

Communication stops until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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

spanning-tree mst cost

Sets the path cost for the applicable Multiple Spanning Tree ports.

Syntax

To set or change information:

spanning-tree mst <mst instance id list> cost <cost>

To delete information:

no spanning-tree mst <mst instance id list> cost

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<mst instance id list>

Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

<cost>

Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 200000000

3. Note on using this parameter:

   Changing the path cost value might change the topology.

Default behavior

The setting of the "spanning-tree cost" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting information by using the "interface range" command, you cannot perform a batch setup of multiple MST instance IDs. Set one MST instance ID. Set one MST instance ID.

spanning-tree mst forward-time

Sets the time required for a Multiple Spanning Tree status transitions.

Syntax

To set or change information:

spanning-tree mst forward-time <seconds>

To delete information:

no spanning-tree mst forward-time

Input mode

```
(config)
```

Parameters

<seconds>

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30

Default behavior

The time required for the status of a port to change is set to 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree mst hello-time

Sets the sending interval of BPDUs in Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst hello-time <hello time>

To delete information:

no spanning-tree mst hello-time

Input mode

```
(config)
```

Parameters

<hello time>

Specifies the sending interval in seconds of BPDUs that are sent regularly from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

3. Note on using this parameter:

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

Default behavior

The sending interval of BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree mst max-age

Sets the maximum valid time of BPDUs that are sent via Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst max-age <seconds>

To delete information:

no spanning-tree mst max-age

Input mode

```
(config)
```

Parameters

<seconds>

Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   6 to 40

3. Note on using this parameter:

   If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree mst max-hops

Sets the maximum-number-of-hops count for BPDUs in Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst max-hops <hop number>

spanning-tree mst <mst instance id list> max-hops <hop number>

To delete information:

no spanning-tree mst max-hops

no spanning-tree mst <mst instance id list> max-hops

Input mode

```
(config)
```

Parameters

<mst instance id list>

Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

   All MST instances are selected.

2. Range of values:

   0 to 4095

<hop number>

Specifies the maximum-number-of-hops count for BPDUs sent by the Switch.

1. Default value when this parameter is omitted:

   20

2. Range of values:

   2 to 40

Default behavior

The maximum-number-of-hops count for BPDUs is set to 20.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree mst port-priority

Sets the priority of the applicable Multiple Spanning Tree ports for each MST instance.

Syntax

To set or change information:

spanning-tree mst <mst instance id list> port-priority <priority>

To delete information:

no spanning-tree mst <mst instance id list> port-priority

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<mst instance id list>

Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

<priority>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The setting of the "spanning-tree port-priority" command is used. If the "spanning-tree port-priority" command has not been set, the port priority is set to 128.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When setting information by using the "interface range" command, you cannot perform a batch setup of multiple MST instance IDs. Set one MST instance ID. Set one MST instance ID.

spanning-tree mst root priority

Sets the bridge priority for each MST instance in Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst <mst instance id list> root priority <priority>

To delete information:

no spanning-tree mst <mst instance id list> root priority

Input mode

```
(config)
```

Parameters

<mst instance id list>

Sets an MST instance ID. One MST instance ID can be set. You can perform a batch setup of multiple MST instance IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 4095

<priority>

Sets the bridge priority. The lower the value, the higher the priority. Use a multiple of 4096 as the bridge priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 61440

3. Note on using this parameter:

   Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree mst transmission-limit

Sets the maximum number of BPDUs that can be sent during each hello-time interval for Multiple Spanning Tree.

Syntax

To set or change information:

spanning-tree mst transmission-limit <count>

To delete information:

no spanning-tree mst transmission-limit

Input mode

```
(config)
```

Parameters

<count>

Sets the maximum number of BPDUs that can be sent per hello-time interval.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree pathcost method

Sets whether to use 16-bit values or 32-bit values as the path cost of ports. This command does not apply to Multiple Spanning Tree but does apply to all other Spanning Tree Protocols (PVST+ and Single Spanning Tree).

When the "spanning-tree vlan pathcost method" command or the "spanning-tree single pathcost method" command is set, the value of the "spanning-tree pathcost method" command is not applied.

If setting of the "spanning-tree cost", "spanning-tree vlan cost", or "spanning-tree single cost" command is omitted, the following value is applied to the path cost according to the interface speed and the "spanning-tree pathcost method" command settings:

- When short is set by the "spanning-tree pathcost method" command:

  10 Mbit/s: 100

  100 Mbit/s: 19

  1 Gbit/s: 4

  2.5 Gbit/s: 3

  10 Gbit/s: 2
- When long is set by the "spanning-tree pathcost method" command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  2.5 Gbit/s: 8000

  10 Gbit/s: 2000

Syntax

To set or change information:

spanning-tree pathcost method { long | short }

To delete information:

no spanning-tree pathcost method

Input mode

```
(config)
```

Parameters

{ long | short }

If long is set, a 32-bit value is used. If short is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

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

   None
3. Note on using this parameter:

- The default value of the path cost changes.
- Changing the path cost value might change the topology.
- If the path cost value is set to 65536 or larger, you cannot change the parameter to short.

Default behavior

short is set by path cost mode.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When mst is set by the "spanning-tree mode" command, a 32-bit value is used for Multiple Spanning Tree. To set a value of 65536 or larger for the path cost using the "spanning-tree cost" command, you must set long for this command.

   You do not need to set this command before setting a path cost value using the "spanning-tree mst cost" command.

spanning-tree port-priority

Sets the port priority of the applicable ports. This command is applied to all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree port-priority <priority>

To delete information:

no spanning-tree port-priority

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<priority>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The settings of the "spanning-tree vlan port-priority", "spanning-tree single port-priority", or "spanning-tree mst port-priority" command are used. If the command described here has not been set, the port priority is set to 128.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree portfast

Sets the PortFast function for the applicable ports. This command is applied to the applicable ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set or change information:

spanning-tree portfast [{ trunk | disable }]

To delete information:

no spanning-tree portfast

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{ trunk | disable }

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

If disable is set, the PortFast function stops.

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

Default behavior

The setting of the "spanning-tree portfast default" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree portfast bpduguard default

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

Syntax

To set information:

spanning-tree portfast bpduguard default

To delete information:

no spanning-tree portfast bpduguard default

Input mode

```
(config)
```

Parameters

None

Default behavior

If the "spanning-tree bpduguard" command is set, that setting is used. If the "spanning-tree bpduguard" command is not set, this command does not work.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree portfast default

Sets the PortFast function to be used by default. This command is valid on the access, protocol, and MAC ports of all Spanning Tree Protocols (PVST+, Single Spanning Tree, and Multiple Spanning Tree).

Syntax

To set information:

spanning-tree portfast default

To delete information:

no spanning-tree portfast default

Input mode

```
(config)
```

Parameters

None

Default behavior

If the "spanning-tree portfast" command has been set, that setting is used. If the "spanning-tree portfast" command has not been set, the "spanning-tree portfast" command does not work.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree single

Starts calculation of the topology for Single Spanning Tree. If the Spanning Tree running mode is PVST+, VLAN 1 is treated as Single Spanning Tree after this command is executed.

Syntax

To set information:

spanning-tree single

To delete information:

no spanning-tree single

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If VLAN 1 was subject to PVST+ before this command was executed, executing this command stops PVST+ for VLAN 1. Removing Single Spanning Tree causes PVST+ to be applied to VLAN 1. If the running mode is Multiple Spanning Tree, Single Spanning Tree does not work.

spanning-tree single cost

Sets the path cost for the applicable Single Spanning Tree ports.

Syntax

To set or change information:

spanning-tree single cost <cost>

To delete information:

no spanning-tree single cost

Input mode

(config-if)

Ethernet interface, port channel interface

Parameters

<cost>

Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   When short is set by the "spanning-tree pathcost method" or the "spanning-tree single pathcost method" command:

   1 to 65535

   When long is set by the "spanning-tree pathcost method" or the "spanning-tree single pathcost method" command:

   1 to 200000000

3. Note on using this parameter:

   Changing the path cost value might change the topology.

Default behavior

The path cost is applied according to the setting of the "spanning-tree single pathcost method" command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree single forward-time

Sets the time required for the status of Single Spanning Tree to change.

Syntax

To set or change information:

spanning-tree single forward-time <seconds>

To delete information:

no spanning-tree single forward-time

Input mode

```
(config)
```

Parameters

<seconds>

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

If stp (802.1D) is set by the "spanning-tree single mode" command, the listening status and the learning status are maintained for the specified period of time. If rapid-stp (802.1w) is set by the "spanning-tree single mode" command, the discarding status and the learning status are maintained for the set period of time (note that this applies only when a timer causes the transition).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30

Default behavior

The time required for the status of a port to change is set to 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree single hello-time

Sets the sending interval of Single Spanning Tree BPDUs.

Syntax

To set or change information:

spanning-tree single hello-time <hello time>

To delete information:

no spanning-tree single hello-time

Input mode

```
(config)
```

Parameters

<hello time>

Specifies the sending interval in seconds of BPDUs that are sent regularly from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

3. Note on using this parameter:

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

Default behavior

The sending interval of BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree single max-age

Sets the maximum valid time of BPDUs that are sent via Single Spanning Tree.

Syntax

To set or change information:

spanning-tree single max-age <seconds>

To delete information:

no spanning-tree single max-age

Input mode

```
(config)
```

Parameters

<seconds>

Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   6 to 40

3. Note on using this parameter:

   If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree single mode

Sets the Single Spanning Tree running mode.

Syntax

To set or change information:

spanning-tree single mode { stp | rapid-stp }

To delete information:

no spanning-tree single mode

Input mode

```
(config)
```

Parameters

{ stp | rapid-stp }

Sets the protocol to be used. If the protocol is changed while using Spanning Tree, the Spanning Tree Protocol is re-initialized. If stp is set, Spanning Tree mode is used. If rapid-stp is set, rapid Spanning Tree mode is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

stp is set for the Single Spanning Tree running mode.

Impact on communication

If the "spanning-tree single" command is set, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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

  2.5 Gbit/s: 3

  10 Gbit/s: 2
- If long is set by the "spanning-tree single pathcost method" command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  2.5 Gbit/s: 8000

  10 Gbit/s: 2000

Syntax

To set or change information:

spanning-tree single pathcost method { long | short }

To delete information:

no spanning-tree single pathcost method

Input mode

```
(config)
```

Parameters

{ long | short }

If long is set, a 32-bit value is used. If short is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

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

   None
3. Note on using this parameter:
   - The default value of the path cost changes.
   - Changing the path cost value might change the topology.
   - When 65536 or a larger value is set for the path cost, you cannot change the parameter to short.

Default behavior

The setting of the "spanning-tree pathcost method" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree single port-priority

Sets the priority for applicable Single Spanning Tree ports.

Syntax

To set or change information:

spanning-tree single port-priority <priority>

To delete information:

no spanning-tree single port-priority

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<priority>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The setting of the "spanning-tree port-priority" command is used. If the "spanning-tree port-priority" command has not been set, the port priority is set to 128.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

spanning-tree single transmission-limit

Sets the maximum number of BPDUs that can be sent during the hello-time interval for Single Spanning Tree.

Syntax

To set or change information:

spanning-tree single transmission-limit <count>

To delete information:

no spanning-tree single transmission-limit

Input mode

```
(config)
```

Parameters

<count>

Sets the maximum number of BPDUs that can be sent per hello-time interval.

This parameter is valid only when rapid-stp (802.1w) is set by the "spanning-tree single mode" command. If stp (802.1D) is set by the "spanning-tree single mode" command, the maximum number of BPDUs that can be sent per second is 3 (fixed) and the setting value of this command is ignored.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree vlan

Configures PVST+. If the "no spanning-tree vlan" command is set after the "spanning-tree single" command has been set, the applicable VLAN works with Single Spanning Tree.

Syntax

To set information:

no spanning-tree vlan <vlan id list>

To delete information:

spanning-tree vlan <vlan id list>

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

3. Note on using this command:

   If the "spanning-tree single" command has been set, VLAN1 does not work in PVST+ mode.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree vlan cost

Sets the path cost for the applicable PVST+ ports.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> cost <cost>

To delete information:

no spanning-tree vlan <vlan id list> cost

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<cost>

Specifies the path cost value. The lower the cost value, the higher the possibility that the port will be used for forwarding the applicable frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   When short is set by the "spanning-tree pathcost method" command or the "spanning-tree vlan pathcost method" command:

   1 to 65535

   When long is set by the "spanning-tree pathcost method" or the "spanning-tree vlan pathcost method" command:

   1 to 200000000

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The method of applying the path cost is determined by the setting of the "spanning-tree vlan pathcost method" command.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. <vlan id list> cannot be specified if the "interface range" command is used to set information.

spanning-tree vlan forward-time

Sets the time required for PVST+ status transition.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> forward-time <seconds>

To delete information:

no spanning-tree vlan <vlan id list> forward-time

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<seconds>

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

If pvst (802.1D) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command, the listening status and the learning status are maintained for the set period of time.

If rapid-pvst (802.1w) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command, the discarding status and the learning status are maintained for the set period of time (note that this applies only when the timer causes the transition).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   4 to 30

Default behavior

The time required for the status of a port to change is set to 15 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree vlan hello-time

Sets the sending interval of PVST+ BPDUs.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> hello-time <hello time>

To delete information:

no spanning-tree vlan <vlan id list> hello-time

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<hello time>

Specifies the sending interval in seconds of BPDUs that are sent regularly from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

3. Note on using this parameter:

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

Default behavior

The sending interval of BPDUs is set to 2.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree vlan max-age

Sets the maximum valid time of BPDUs that are sent via PVST+.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> max-age <seconds>

To delete information:

no spanning-tree vlan <vlan id list> max-age

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<seconds>

Sets the maximum valid time in seconds for BPDUs that are sent from the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   6 to 40

3. Note on using this parameter:

   If you set a value less than 20, then this might result in a changeable topology.

Default behavior

The maximum valid time of BPDUs that can be sent from a Switch is set to 20 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree vlan mode

Sets the PVST+ running mode.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> mode { pvst | rapid-pvst }

To delete information:

no spanning-tree vlan <vlan id list> mode

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

{ pvst | rapid-pvst }

Sets the protocol to be used. If the protocol is changed while using Spanning Tree, the Spanning Tree Protocol is re-initialized. If pvst is set, PVST+ mode is used. If rapid-pvst is set, rapid PVST+ mode is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The PVST+ running mode is set by the "spanning-tree mode" command.

Impact on communication

If pvst or rapid-pvst has been specified by the "spanning-tree mode" command, communications are interrupted until recalculation of the topology is complete.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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

  2.5 Gbit/s: 3

  10 Gbit/s: 2
- When long is set by the "spanning-tree vlan pathcost method" command:

  10 Mbit/s: 2000000

  100 Mbit/s: 200000

  1 Gbit/s: 20000

  2.5 Gbit/s: 8000

  10 Gbit/s: 2000

Syntax

To set or change information:

spanning-tree vlan <vlan id list> pathcost method { long | short }

To delete information:

no spanning-tree vlan <vlan id list> pathcost method

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

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

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

{ long | short }

If long is set, a 32-bit value is used. If short is set, a 16-bit value is used.

1. Default value when this parameter is omitted:

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

None

3. Note on using this parameter:
   - The default value of the path cost changes.
   - Changing the path cost value might change the topology.
   - When 65536 or a larger value is set for the path cost, you cannot change the parameter to short.

Default behavior

The setting of the "spanning-tree pathcost method" command is used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree vlan port-priority

Sets the priority for the applicable PVST+ ports.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> port-priority <priority>

To delete information:

no spanning-tree vlan <vlan id list> port-priority

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<priority>

Sets the port priority. Use a multiple of 16 as the port priority. The lower the value, the higher the priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 240

3. Note on using this parameter:

   Changing the port priority might change the topology.

Default behavior

The setting of the "spanning-tree port-priority" command is used. If the "spanning-tree port-priority" command has not been set, the port priority is set to 128.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. <vlan id list> cannot be specified if the "interface range" command is used to set information.

spanning-tree vlan priority

Sets the PVST+ bridge priority.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> priority <priority>

To delete information:

no spanning-tree vlan <vlan id list> priority

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<priority>

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

Use a multiple of 4096 as the bridge priority.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 61440

3. Note on using this parameter:

   Changing the bridge priority might change the topology.

Default behavior

The bridge priority is set to 32768.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

spanning-tree vlan transmission-limit

Sets the maximum number of BPDUs that can be sent within the PVST+ hello-time interval.

Syntax

To set or change information:

spanning-tree vlan <vlan id list> transmission-limit <count>

To delete information:

no spanning-tree vlan <vlan id list> transmission-limit

Input mode

```
(config)
```

Parameters

<vlan id list>

Starts configuration of PVST+ for the set VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

<count>

Sets the maximum number of BPDUs that can be sent per hello-time interval.

This parameter is effective only when rapid-pvst (802.1w) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command. When pvst (802.1D) is set by the "spanning-tree mode" command or the "spanning-tree vlan mode" command, the maximum number of BPDUs that can be sent per second is 3 (fixed) and the value set by this command is ignored.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of BPDUs that can be sent is set to 3.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

19 Ring Protocol

axrp

Set a ring ID. In addition, to collect information necessary for the Ring Protocol function, switches to config-axrp mode. A maximum of 24 ring IDs can be set for a Switch.

If this setting is removed, the ring information that is already set for ring IDs is deleted.

Syntax

To set information:

axrp <ring id>

To delete information:

no axrp <ring id>

Input mode

```
(config)
```

Parameters

<ring id>

Sets the ring ID.

The same ring ID must be specified for all devices belonging to the same ring. Specify a unique ring ID for each different ring in a network.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

axrp vlan-mapping

Sets the VLAN mapping to be applied to a VLAN group and also the VLANs that participate in VLAN mapping.

Syntax

To set or change information:

axrp vlan-mapping <mapping id> vlan <vlan id list>

To change information:

axrp vlan-mapping <mapping id> {vlan <vlan id list> | vlan add <vlan id list> | vlan remove <vlan id list>}

To delete information:

no axrp vlan-mapping <mapping id>

Input mode

```
(config)
```

Parameters

<mapping id>

Specifies the VLAN mapping ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 128

vlan <vlan id list>

Sets the VLANs that participate in VLAN mapping. When specifying multiple VLANs, you can specify a range.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

vlan add <vlan id list>

Specifies the VLANs to be added to the VLAN list you have configured.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

vlan remove <vlan id list>

Specifies the VLANs to be removed from the VLAN list you have configured.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

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

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify multiple VLAN mappings for one VLAN.
2. You cannot specify a VLAN mapping for a VLAN that is used as the control VLAN.
3. You cannot specify a VLAN mapping for a VLAN that is used as the multi-fault monitoring VLAN.

axrp-ring-port

Sets an interface to be used as the ring port for the Ring Protocol. The interfaces that can be set are Ethernet interfaces and port channel interfaces.

Syntax

To set or change information:

axrp-ring-port <ring id> [shared]

To delete information:

no axrp-ring-port <ring id>

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<ring id>

Sets the ring ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

shared

When a Switch serves as a transit node on a shared link, this parameter specifies the ring port that will be the shared link.

Two ports must be specified to correspond with the ring ID.

1. Default value when this parameter is omitted:

   The interface serves as a standard ring port.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Two ring ports can be specified as corresponding to one ring ID.
2. 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.

control-vlan

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

Setting the forwarding-delay-time parameter for a transit node allows you to set the time required to transfer the status of the control VLAN to Forwarding during initialization. You can therefore adjust the time required before starting to monitor the status of received flush control frames on the transit node, to ensure that flush control frames sent by the master node are received.

Syntax

To set or change information:

control-vlan <vlan id> [forwarding-delay-time <seconds>]

To delete information:

no control-vlan

Input mode

```
(config-axrp)
```

Parameters

<vlan id>

Specify the VLAN to be used as the control VLAN.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

   Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

forwarding-delay-time <seconds>

Sets the time (in seconds) required before the status of the control VLAN changes to Forwarding when the transit node device is started or when the Ring Protocol program is restarted.

1. Default value when this parameter is omitted:

   The control VLAN transitions to Forwarding immediately after the ring port comes up.

2. Range of values:

   1 to 65535

3. Note on using this parameter:

   To delete only this parameter, set control-vlan again with this parameter omitted. This operation is used to delete parameters.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify a VLAN that is used as a control VLAN by another ring ID.
2. You cannot specify a VLAN that is used in a VLAN group.
3. For the control VLAN, you cannot specify a VLAN that is being used by the multi-fault monitoring VLAN.
4. While the Ring Protocol is operating, if you change or delete the control VLAN, this function is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.
5. forwarding-delay-time takes effect when the following occurs:
   - The Switch is started (includes execution of the "reload" or "ppupdate" operation command).
   - A Ring Protocol program is restarted (including execution of the "restart axrp" operation command).

disable

Disables the Ring Protocol function.

Syntax

To set information:

disable

To delete information:

no disable

Input mode

```
(config-axrp)
```

Parameters

None

Default behavior

The Ring Protocol function is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If this command is entered while the Ring Protocol is operating, the Ring Protocol function is disabled. In this case, a loop might occur depending on a network configuration (ring configuration) to which the Ring Protocol function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.

forwarding-shift-time

For a transit node, sets the reception hold time for flush control frames.

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

Syntax

To set or change information:

forwarding-shift-time {<seconds> | infinity}

To delete information:

no forwarding-shift-time

Input mode

```
(config-axrp)
```

Parameters

{<seconds> | infinity}

For a transit node, specifies the hold time in seconds before a flush control frame is received.

If you set "infinity", there is no limit on the hold time, and the status of the ring port on the transit node does not switch to Forwarding until a flush control frame is received.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535 (seconds) or infinity

Default behavior

For a transit node, 10 seconds is used as the reception hold time for flush control frames.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the sending interval for health-check frames on the master node is longer than the reception hold time for flush control frames on the transit node, the status of the ring port on the transit node switches to Forwarding before the master node detects the normal status. This could produce a temporary loop.

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

mac-clear-mode

Specifies MAC address table entries to be cleared when a ring failure occurs or is recovered.

Syntax

To set information:

mac-clear-mode system

To delete information:

no mac-clear-mode

Input mode

```
(config-axrp)
```

Parameters

system

Clears all entries in the MAC address table when a ring failure occurs or is recovered.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

MAC address table entries are cleared for each ring port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

mode

Sets the running mode of the Switch used for the ring.

In addition, if the ring configuration is a multi-ring configuration with shared links, sets the attributes of a ring configured by Switches, and the positioning of the Switches in the ring.

Syntax

To set or change information:

mode transit

To delete information:

no mode

Input mode

```
(config-axrp)
```

Parameters

transit

Serves as a transit node.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If you change or delete the mode while Ring Protocol is used, the function is temporarily disabled. As a result, a loop might occur depending on the network configuration (ring configuration) to which the function is applied. To avoid a loop, before entering this command, place the interface that is the ring port in the shutdown state.

multi-fault-detection mode

Sets the multi-fault monitoring mode for shared link monitoring rings.

Set this command for a ring whose ring ID is the same as that of the shared link monitoring ring of the shared node in a multi-ring configuration with shared links.

Syntax

To set or change information:

multi-fault-detection mode transport-only

To delete information:

no multi-fault-detection mode

Input mode

```
(config-axrp)
```

Parameters

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:

   None

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

None

multi-fault-detection vlan

Sets the VLAN for multi-fault monitoring. The VLAN specified for this command is used to send and receive control frames used for multi-fault monitoring.

Set this command for shared link monitoring rings in a multi-ring configuration with shared links.

Syntax

To set or change information:

multi-fault-detection vlan <vlan id>

To delete information:

no multi-fault-detection vlan

Input mode

```
(config-axrp)
```

Parameters

vlan <vlan id>

Specifies a VLAN to be used for multi-fault monitoring.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters". Note that the default VLAN (VLAN ID = 1) cannot be specified for this parameter.

Default behavior

Multi-fault monitoring for shared link monitoring rings is not performed.

Impact on communication

None

When the change is applied:

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify a VLAN that is used as a multi-fault monitoring VLAN by another ring ID.
2. You cannot specify a VLAN that is used as a control VLAN as the multi-fault monitoring VLAN.
3. You cannot specify a VLAN that is used in VLAN mapping.

name

Sets the name for identifying a ring.

Syntax

To set or change information:

name <name>

To delete information:

no name

Input mode

```
(config-axrp)
```

Parameters

<name>

Sets the name for identifying a ring.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string of no more than 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

NULL is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

vlan-group

Sets the VLAN group that will be used for the Ring Protocol and the mapping IDs of the VLANs participating in the VLAN groups.

A maximum of two VLAN groups can be set for a ring. In addition, by creating two VLAN groups, loads can be balanced between the two VLANs.

Syntax

To set or change information:

vlan-group <group id> vlan-mapping <mapping id list>

To delete information:

no vlan-group <group id>

Input mode

```
(config-axrp)
```

Parameters

<group id>

Specifies the VLAN group ID that will be used for the Ring Protocol.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 2

vlan-mapping <mapping id list>

Specifies the mapping IDs of the VLANs participating in a VLAN group. One VLAN mapping ID can be set. You can perform a batch setup of multiple VLAN mapping IDs using hyphens (-) and commas (,).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 128

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the same VLAN mapping is assigned to VLAN groups in different rings, these rings cannot share the same port as a ring port. Note, however, that it is possible to share the same ring port if it is a shared link ring port (a ring port for which shared is specified).

20 IGMP snooping

ip igmp snooping (global)

Suppresses the IGMP snooping function on a Switch.

Syntax

To set information:

no ip igmp snooping

To delete information:

ip igmp snooping

Input mode

```
(config)
```

Parameters

None

Default behavior

The IGMP snooping function is enabled on a Switch.

Impact on communication

The IGMP snooping function stops.

When the change is applied

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

Notes

1. If the "no ip igmp snooping" command is set, IGMP snooping is disabled on the Switch. Therefore, setting the "ip igmp snooping" command on a VLAN interface does not enable IGMP snooping on the interface.

ip igmp snooping (VLAN interface)

Enables the IGMP snooping function on a VLAN interface.

Syntax

To set information:

ip igmp snooping

To delete information:

no ip igmp snooping

Input mode

`(config-if)`

VLAN interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. If the "no ip igmp snooping" command is set in global configuration mode, IGMP snooping is disabled on the Switch. Therefore, setting this command does not enable IGMP snooping on the interface.

ip igmp snooping fast-leave

Immediately stops multicast communication to the applicable port if IGMP Leave and IGMPv3 Report (leave request) messages are received on a VLAN interface.

Syntax

To set information:

ip igmp snooping fast-leave

To delete information:

no ip igmp snooping fast-leave

Input mode

```
(config-if)
```

VLAN interface

Parameters

None

Default behavior

If IGMP Leave and IGMPv3 Report (leave request) messages are received, make sure there are no members from the same multicast group on the applicable port, and then stop multicast communication. Multicast communication will continue (for a default value of three seconds) for the check process after IGMP Leave and IGMPv3 Report (leave request) messages are received.

Impact on communication

None

When the change is applied

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

Notes

1. Immediately stops multicast communication to the applicable port if you set this command and receive IGMP Leave and IGMPv3 Report (leave request) messages. For this reason, if there are members from the same multicast group on the applicable port, multicast communication to the applicable members stops temporarily. In this case, multicast communication is restarted when an IGMP Report (membership request) message is received again from the applicable member.

ip igmp snooping mrouter

Specifies a multicast router port on a VLAN interface.

Syntax

To set information:

ip igmp snooping mrouter interface <interface type> <interface number>

To delete information:

no ip igmp snooping mrouter interface <interface type> <interface number>

Input mode

```
(config-if)
```

VLAN interface

Parameters

<interface type> <interface number>

Specifies an interface for which a multicast router port is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

   - Ethernet interface
   - Port channel interface

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. If ip igmp snooping is not specified for the applicable interface, this function does not work.
2. Some of ports with port channel interfaces set cannot be specified as multicast router ports. If you do so, the applicable port becomes invalid.

ip igmp snooping mrouter discovery

Set the monitoring packet type for detecting multicast routers on the VLAN interface. If multicast router is detected, the port to which the target VLAN belongs is dynamically set as a multicast router port.

Syntax

To set information:

ip igmp snooping mrouter discovery igmp

ip igmp snooping mrouter discovery pim

To delete information:

no ip igmp snooping mrouter discovery igmp

no ip igmp snooping mrouter discovery pim

Input mode

```
(config-if)
```

VLAN interface

Parameters

igmp

Monitor IGMP packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

pim

Monitor PIM packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Neither IGMP packets nor PIM packets are monitored.

Impact on communication

None

When the change is applied

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

Notes

1. If you delete this command, the multicast router information detected on the port to which the target VLAN belongs will be cleared.

ip igmp snooping mrouter discovery extension

Set the increment for the retention time of multicast router information.

Syntax

To set or change information:

ip igmp snooping mrouter discovery extension <seconds>

To delete information:

no ip igmp snooping mrouter discovery extension

Input mode

```
(config)
```

Parameters

<seconds>

Specify the increment for the retention time of detected multicast router information in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 86400 (seconds)

Default behavior

The increment of retention time becomes 0.

Impact on communication

None

When the change is applied

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

Notes

None

ip igmp snooping mrouter logging

When "no ip igmp snooping mrouter logging" is set, the output of operation messages related to multicast router detection is suppressed.

Syntax

To set information:

```
no ip igmp snooping mrouter logging
```

To delete information:

```
ip igmp snooping mrouter logging
```

Input mode

```
(config)
```

Parameters

None

Default behavior

Outputs operation message related to multicast router detection.

Impact on communication

None

When the change is applied

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

Notes

None

ip igmp snooping querier

Enables the IGMP querier function on a VLAN interface.

Syntax

To set information:

ip igmp snooping querier

To delete information:

no ip igmp snooping querier

Input mode

`(config-if)`

VLAN interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. If ip igmp snooping is not specified for the applicable interface or the IP address is not set, the querier function does not work.

ip igmp snooping query-interval

Sets the sending interval at which IGMP query messages are periodically sent from the Switch on the VLAN interface.

Syntax

To set or change information:

ip igmp snooping query-interval <seconds>

To delete information:

no ip igmp snooping query-interval

Input mode

(config-if)

VLAN interface

Parameters

<seconds>

Specify the sending interval of query messages in seconds.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 300 (seconds)

Default behavior

It works in 125 seconds.

Impact on communication

If you change this command while the IGMP querier function is in operation, the group information may temporarily time out.

When the change is applied

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

Notes

1. When operating with IGMPv2, use this command to set the sending interval of IGMP query message to the same value within the target VLAN that includes other devices.

21 MLD snooping

ipv6 mld snooping (global)

Suppresses the MLD snooping function on a Switch.

Syntax

To set information:

no ipv6 mld snooping

To delete information:

ipv6 mld snooping

Input mode

```
(config)
```

Parameters

None

Default behavior

The MLD snooping function is enabled on a Switch.

Impact on communication

The MLD snooping function stops.

When the change is applied

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

Notes

1. If no ipv6 mld snooping is set, MLD snooping is disabled on the Switch. Therefore, setting the "ipv6 mld snooping" command on a VLAN interface does not enable MLD snooping on the interface.

ipv6 mld snooping (VLAN interface)

Enables the MLD snooping function on a VLAN interface.

Syntax

To set information:

ipv6 mld snooping

To delete information:

no ipv6 mld snooping

Input mode

(config-if)

VLAN interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. If the "no ipv6 mld snooping" command is set in global configuration mode, MLD snooping is disabled on the Switch. Therefore, setting this command does not enable MLD snooping on the interface.

ipv6 mld snooping mrouter

Specifies a multicast router port on a VLAN interface.

Syntax

To set information:

ipv6 mld snooping mrouter interface <interface type> <interface number>

To delete information:

no ipv6 mld snooping mrouter interface <interface type> <interface number>

Input mode

```
(config-if)
```

VLAN interface

Parameters

<interface type> <interface number>

Specifies an interface for which a multicast router port is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

   - Ethernet interface
   - Port channel interface

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. If ipv6 mld snooping is not specified for the applicable interface, this function does not work.
2. Some of ports with port channel interfaces set cannot be specified as multicast router ports. If you do so, the applicable port becomes invalid.

ipv6 mld snooping querier

Enables the MLD querier function on a VLAN interface.

Syntax

To set information:

ipv6 mld snooping querier [<ipv6 address>]

To delete information:

no ipv6 mld snooping querier

Input mode

```
(config-if)
```

VLAN interface

Parameters

<ipv6 address>

Set the source IPv6 address of the MLD query message sent by the MLD querier function.

1. Default value when this parameter is omitted:

   The MLD querier function is disabled.

2. Range of values:

   Specify an IPv6 link-local addresses in colon notation.

Default behavior

None

Impact on communication

None

When the change is applied

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

Notes

1. If ipv6 mld snooping is not specified for the applicable interface or the IPv6 address is not set, the MLD querier function does not work.

22 IPv4 Communication

arp

This command creates a static ARP table. If a product that does not support ARP is connected, conversion is not possible between an IPv4 address and 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> [interface vlan <vlan id>]

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.

interface vlan <vlan id>

Specifies a VLAN ID.

1. Default value when this parameter is omitted:

   To set or change information:

   This parameter cannot be omitted.

   To delete information:

   This parameter cannot be omitted if there are multiple static ARP entries that have the same next-hop IPv4 address.

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 ffff.ffff.ffff

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

arp max-send-count

This command specifies the maximum number of times an ARP request packet is sent.

Syntax

To set or change information:

arp max-send-count <count>

To delete information:

no arp max-send-count

Input mode

(config-if)

VLAN interface

Parameters

<count>

Specifies the maximum number of times an ARP request packet is 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 maximum number of times an ARP request frame is sent is set to 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

arp send-interval

This command specifies the retry interval for sending an ARP request packet.

Syntax

To set or change information:

arp send-interval <seconds>

To delete information:

no arp send-interval

Input mode

(config-if)

VLAN interface

Parameters

<seconds>

Specifies the retry interval for sending an ARP request packet.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10 (seconds)

Default behavior

The retry interval for sending an ARP request packet is set to 2 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

arp timeout

This command specifies the aging time for an ARP cache table.

Syntax

To set or change information:

arp timeout <seconds>

To delete information:

no arp timeout

Input mode

(config-if)

VLAN interface

Parameters

<seconds>

Specifies the aging time for an ARP cache table.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   60 to 86400 (seconds)

Default behavior

14400 seconds (4 hours) is set as the aging time for an ARP cache table.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip address

This command specifies 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)`

VLAN interface

Parameters

<ip address>

Specifies the local IPv4 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

<subnet mask>

Specifies 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 255.255.255.255 (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

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To change the IPv4 address, delete the already set IPv4 address and then set a new IPv4 address.

ip mtu

This command specifies the MTU length of IP packets sent on the interface.

Syntax

To set or change information:

ip mtu <length>

To delete information:

no ip mtu

Input mode

(config-if)

VLAN interface

Parameters

<length>

Specifies the MTU length of IP packets sent on the 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 the "mtu" command.

Check the IP MTU length you are using by using the "show ip interface" operation command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   128 to 9216 (bytes)

Default behavior

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.

ip route

Set the IPv4 static route.

Syntax

To set information:

ip route <ipv4 prefix> <mask> <nexthop address>

To delete information:

no ip route <ipv4 prefix> <mask> <nexthop address>

Input mode

```
(config)
```

Parameters

<ipv4 prefix>

Specifies the destination IPv4 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv4 address.

   Note: For <ipv4 prefix>, set 0 to the bits outside the range of <mask>.

<mask>

Specifies the netmask of the IPv4 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv4 address mask.

   Note: Specify the address mask so that when it is converted to a binary number, all bits after the first bit that is 0 are set to 0.

<nexthop address>

Specifies the next hop address of the route.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv4 address.

Default behavior

IPv4 static routes are not generated.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

23 IPv6 Communication

ipv6 address

The "ipv6 address" command sets the local IPv6 address.

Syntax

To set or change information:

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

ipv6 address <ipv6 address> link-local

To delete information:

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

no ipv6 address <ipv6 address>

Input mode

`(config-if)`

VLAN interface

Parameters

<ipv6 address>

The "ipv6 address" command sets the local IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv6 global address or IPv6 link-local address in colon notation.

<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. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify the IPv6 prefix format in which all bits of the interface ID of the IPv6 address are set to 0. However, you cannot specify fe80::0.

/<prefixlen>

Specifies the prefix length.

1. Default value when this parameter is omitted:

   64

2. Range of values:

   Specify 1 to 128.

link-local

Overwrites the link-local address that is automatically created by the "ipv6 enable" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

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 enable

Specify this command when using IPv6 addresses.

This command automatically creates a link address.

Syntax

To set information:

ipv6 enable

To delete information:

no ipv6 enable

Input mode

`(config-if)`

VLAN interface

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

ipv6 icmp error-interval

The "ipv6 icmp error-interval" command specifies the sending interval of ICMPv6 error messages.

Syntax

To set or change information:

ipv6 icmp error-interval <milli seconds>

To delete information:

no ipv6 icmp error-interval

Input mode

```
(config)
```

Parameters

<milli seconds>

Sets the minimum time between ICMP error messages. If you specify 0, the interval between the sending of ICMP error packets is not limited to the specified or default interval for sending error messages.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 2147483647 (milliseconds)

Default behavior

The sending interval of ICMPv6 error messages is set to 1000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The actual transmission interval may be approximately 1/2 to 1/16 of the setting value, depending on the prefix length of the destination route to which ICMPv6 errors are sent.

ipv6 nd accept-ra

Receives router advertisement messages and automatically generates stateless addresses.

Syntax

To set or change information:

ipv6 nd accept-ra [default-gateway]

To delete information:

no ipv6 nd accept-ra

Input mode

```
(config-if)
```

VLAN interface

Parameters

default-gateway

Adds a default route with the next hop address as the source address of the received router advertisement message.

1. Default value when this parameter is omitted:

   Does not add the default route.

2. Range of values:

   None

Default behavior

Stateless address automatic generation based on the router advertisement message reception will not be performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The IPv6 address and default route that are automatically generated from router advertisement messages on the interface where this command is set remain until their lifetime expires even after the settings of this command are changed or deleted. If you want to delete the automatically generated IPv6 address and default route immediately after changing or deleting the settings, take the interface down and then bring it up again.
2. If the default-gateway parameter is specified on multiple interfaces, or if multiple routers exist on the interface for which the default-gateway parameter is set and multiple router advertisement messages are received, multiple default routes are generated. The default route selected is determined by the order in which they are added and the state of the next hop address router.

3. If this command is specified on multiple interfaces and routers on each interface distribute the same prefix information in router advertisement messages, IPv6 addresses with the same prefix will be generated on different interfaces. Additionally, if you receive a router advertisement message distributing the same prefix as the IPv6 address prefix manually set using the "ipv6 address" command, multiple IPv6 addresses with the same prefix may exist. In either case, check the settings of the router that distributes router advertisement messages to make sure there are no errors in the network configuration.
4. Even if a router advertisement message containing new prefix information is received with seven or more IPv6 global addresses set on an interface by manual configuration using the "ipv6 address" command or by receiving a router advertisement message, the IPv6 address for that prefix will not be automatically generated. Manual IPv6 global address settings using the "ipv6 address" command can be configured for up to seven addresses per interface, regardless of the number of addresses automatically set using router advertisement messages.
5. Even if an address for new prefix information cannot be generated due to the upper limit on the number of addresses per interface, a directly connected route for the target prefix is generated. Configure the router to not distribute router advertisement messages beyond the upper limit.

ipv6 neighbor

The "ipv6 neighbor" command 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> [interface vlan <vlan id>]

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.

interface vlan <vlan id>

Specifies a VLAN ID.

1. Default value when this parameter is omitted:

   To set or change information:

   This parameter cannot be omitted.

   To delete information:

   This parameter cannot be omitted if there are multiple static NDP entries that have the same next-hop IPv6 address.

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 lowest 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

ipv6 route

The "ipv6 route" command generates an IPv6 static route.

Syntax

To set or change information:

ipv6 route <ipv6 prefix>/<prefix len> <nexthop address> [<interface type> <interface number>]

To delete information:

no ipv6 route <ipv6 prefix>/<prefix len> <nexthop address> [<interface type> <interface number>]

Input mode

```
(config)
```

Parameters

<ipv6 prefix>

Specifies the destination IPv6 prefix.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <ipv6 prefix>, specify an IPv6 prefix.

   Note: Set all the bits following the bits specified for <prefix len> of <ipv6 prefix> to 0.

<prefix len>

Specifies the prefix length.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 0 to 128 in decimal.

<nexthop address>

Specifies the IPv6 next hop address. When you specify an IPv6 link-local address, specify the interface after this parameter.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv6 global address, IPv6 site-local address, or IPv6 link-local address.

<interface type> <interface number>

Specifies the interface used for resolving the next hop.

If an IPv6 link-local address is specified for <nexthop address>, specify the interface with this parameter.

1. Default value when this parameter is omitted:

   The interface used for resolving the next hop is not specified.

2. Range of values:

For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

- VLAN interface

Default behavior

IPv6 static routes are not generated.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Only the address of a neighboring device that has the same prefix as the address set for the interface of the Switch can be set as the next hop address.

24 Loopback Interface

interface loopback

This command moves to the loopback interface level.

Syntax

To set information:

interface loopback 0

To delete information:

no interface loopback 0

Input mode

```
(config)
```

Parameters

0

Specifies a loopback interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip address (loopback)

This command specifies a loopback interface IP address.

Syntax

To set information:

ip address <ip address>

To delete information:

no ip address

Input mode

(config-if)

Loopback interface

Parameters

<ip address>

Specifies an IPv4 address for a loopback interface. You can specify only one IPv4 address. Even if you specify multiple addresses, only the last specified address is applied.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

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 address (loopback)

The "ipv6 address" command specifies an IPv6 address for a loopback interface.

You can specify this command regardless of the "ipv6 enable" command setting.

Syntax

To set information:

ipv6 address <ipv6 address>

To delete information:

no ipv6 address

Input mode

`(config-if)`

Loopback interface

Parameters

<ipv6 address>

Specify an IPv6 address for a loopback interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv6 global address in colon notation. You can specify only one IPv6 address. Even if you specify multiple addresses, only the last specified address is applied. An IPv6 link-local address cannot be specified.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

25 DHCP Server Function

client-name

The "client-name" command specifies the host name option for a client. The host name specified by this command is used by the client when the DHCP server distributes a static IP address to the client.

Syntax

To set or change information:

client-name <Host Name>

To delete information:

no client-name

Input mode

```
(dhcp-config)
```

Parameters

<Host Name>

Specifies the name of a client. For the restrictions of characters, see RFC 1035.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A host name that contains a maximum of 14 characters

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

default-router

The "default-router" command specifies the router option for a client. This option is a list of IP addresses that can be used by clients as the router IP address (default router) on the subnet.

Syntax

To set or change information:

default-router <IP Address> [<IP Address>...]

To delete information:

no default-router

Input mode

```
(dhcp-config)
```

Parameters

<IP Address> [<IP Address>...]

Specifies one or more router IP addresses for the subnet of a client (default router). The routers are specified according to the priority, starting from the higher ones on the left.

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

Default behavior

None (The Switches do not distribute a list of router IP addresses to the client when the client requests a router IP address. However, the Switches insert the IP address set for the client in the router IP address field and distribute the information to the client.)

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 configured for the server is 16 per DHCP address pool.

dns-server

The "dns-server" command specifies the DNS server options for a client. This DNS server option is a list of DNS server IP addresses that can be used by clients.

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> [<IP Address>...]

Specifies the IP address of a DNS server that a client can use. The server addresses are specified according to the priority, starting from the higher ones on the left.

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

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The maximum number of IP addresses that can be configured for the server is 16 per DHCP address pool.

domain-name

The "domain-name" command specifies the domain name option for a client. The domain name specified by using this command is used by the client as the preferred domain name and DNS resolves it to the IP address distributed to the client.

Syntax

To set or change information:

domain-name <Domain Name>

To delete information:

no domain-name

Input mode

```
(dhcp-config)
```

Parameters

<Domain Name>

Specifies the domain name to be used by the client when DNS is used to resolve the host name for the distributed IP address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A domain name that contains a maximum of 253 characters

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

hardware-address

The "hardware-address" command 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.

host

The "host" command specifies the static IP address to be assigned to a client when a static IP address is distributed to the 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 25-1: IP address range for each class

Class	IP address
Class A (/8)	1.x.x.x to 127.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> | /<Masklen>}

1. Default value when this parameter is omitted:
   A mask corresponding to class A, B, or C
2. Range of values:
   For <Mask>, specify a value in the range from 255.0.0.0 to 255.255.255.255.
   For <Masklen>, specify a value in the range from 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 DHCP address 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 DHCP address pool cannot be provided.
3. When the "host" command is set, the optional information (set by the "client-name", "default-router", "dns-server", "domain-name", "netbios-name-server", and "netbios-node-type" 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.

ip dhcp dynamic-dns-update

The "ip dhcp dynamic-dns-update" command specifies whether to link dynamic DNS when distributing IP addresses.

Syntax

To set information:

ip dhcp dynamic-dns-update

To delete information:

no ip dhcp dynamic-dns-update

Input mode

```
(config)
```

Parameters

None

Default behavior

DNS is not updated.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip dhcp excluded-address

The "ip dhcp excluded-address" command specifies the range of IP addresses in the DHCP address pool specified by using the "network" command that are to be excluded from distribution.

Syntax

To set 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>]

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

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

Default behavior

All IP addresses in the range specified 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. If the number of DHCP address pools exceeds the maximum number when the setting for excluded addresses is deleted, you cannot delete the setting.

ip dhcp key

The "ip dhcp key" command sets the authentication key to be used for authentication on the DNS server when dynamic DNS is used.

Syntax

To set or change information:

ip dhcp key <Key Name> [secret-hmac-md5 <Key>]

To delete information:

no ip dhcp key <Key Name>

Input mode

```
(config)
```

Parameters

<Key Name>

Sets the key name required for authentication on the dynamic DNS server. This name must be the same as the key name set on the dynamic DNS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A name that contains a maximum of 63 characters

secret-hmac-md5 <Key>

Specifies the shared key created on the dynamic DNS server side. Use double quotation marks to enclose the key. The Switch supports only the keys generated by HMAC-MD5.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   A string consisting of a maximum of 90 characters, including double quotation marks (") (the string cannot contain a space)

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 key parameter is set for the "ip dhcp zone" command, you cannot delete the ip dhcp key setting. You need to first delete the ip dhcp zone setting, and then delete the ip dhcp key setting.

ip dhcp pool

The "ip dhcp pool" command sets DHCP address pool information.

Syntax

To set information:

ip dhcp pool <Pool Name>

To delete information:

no ip dhcp pool <Pool Name>

Input mode

```
(config)
```

Parameters

<Pool Name>

Specifies 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:

   A name that contains a maximum of 14 characters

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can set this command to the sum of the maximum number of managed subnets and the maximum number of static IP addresses.

ip dhcp zone

The "ip dhcp zone" command sets the information about the zone where DNS updating is performed when a dynamic DNS server is linked.

Syntax

To set or change information:

ip dhcp zone <Zone Name> [primary <IP Address>] [key <Key Name>]

To delete information:

no ip dhcp zone <Zone Name>

Input mode

```
(config)
```

Parameters

<Zone Name>

Specifies a DNS zone name for the domain for normal or reverse lookup. Here, the zone name must end with a dot (.).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   A zone name that contains a maximum of 254 characters

primary <IP Address>

Specifies the IP address of the dynamic DNS server that is to be set automatically.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   The following addresses cannot be set:

   - 127.0.0.0 to 127.255.255.255
   - Addresses that do not belong to class A, B, or C

key <Key Name>

Specifies the key name set in the DHCP dynamic DNS key information.

1. Default value when this parameter is omitted:

   None

2. Range of values:

   A name that contains a maximum of 63 characters

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Before you attempt to specify the key parameter in the "ip dhcp zone" command, you need to use the "ip dhcp key" command to set the key.

lease

The "lease" command specifies the default lease time for the IP address distributed to a client.

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}

Sets the lease time.

<time day> [<time hour> [<time min> [<time sec>]]]

Specify the lease time in days, hours, minutes, and seconds. Note that values smaller than 10 seconds cannot be set. Specify a value in the range from 10 seconds to 365 days.

infinite

Specifies an unlimited lease time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <time day>, specify a value in the range from 0 to 365. The remaining items can be omitted.

   For <time hour>, specify a value in the range from 0 to 23. The remaining items can be omitted.

   For <time min>, specify a value in the range from 0 to 59. The remaining items can be omitted.

   For <time sec>, specify a value in the range from 0 to 59.

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 assigned 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 DHCP address 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 very limited cases such as temporary IP addresses that will be used only for a short period of time. Also, make sure that the client can work reliably if a short lease time is set.

max-lease

The "max-lease" command specifies the maximum lease time allowed when a client requests an IP address with a specific lease time.

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}

Specifies the maximum lease time when a client specifies a time.

<time day> [<time hour> [<time min> [<time sec>]]]

Specifies the maximum lease time in days, hours, minutes, and seconds. Note that values smaller than 10 seconds cannot be set. Specify a value in the range from 10 seconds to 365 days.

infinite

Specifies the maximum lease time as unlimited.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <time day>, specify a value in the range from 0 to 365. The remaining items can be omitted.

   For <time hour>, specify a value in the range from 0 to 23. The remaining items can be omitted.

   For <time min>, specify a value in the range from 0 to 59. The remaining items can be omitted.

   For <time sec>, specify a value in the range from 0 to 59.

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 maximum 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 DHCP address 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 very limited cases such as temporary IP addresses that will be used only for a short period of time. Also, make sure that the client can work reliably if a short lease time is set.

netbios-name-server

The "netbios-name-server" command specifies the NetBIOS name server options (NBNS/WINS servers) for a client. The NetBIOS name server option is a list of IP addresses of NetBIOS name servers (NBNS/WINS servers) that can be used by clients.

Syntax

To set or change information:

netbios-name-server <IP Address> [<IP Address>...]

To delete information:

no netbios-name-server

Input mode

```
(dhcp-config)
```

Parameters

<IP Address> [<IP Address>...]

Specifies the IP address of a NetBIOS name server (NBNS/WINS server). The server addresses are specified according to the priority, starting from the higher ones on the left.

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

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The maximum number of IP addresses that can be configured for the server is 16 per DHCP address pool.

netbios-node-type

The "netbios-node-type" command specifies the NetBIOS node type option for a client. A NetBIOS node type indicates the name resolution method used by the client when NetBIOS over TCP/IP is used.

Syntax

To set or change information:

netbios-node-type {b-node | p-node | m-node | h-node}

To delete information:

no netbios-node-type

Input mode

```
(dhcp-config)
```

Parameters

{b-node | p-node | m-node | h-node}

Specifies the node type of the NetBIOS over TCP/IP client (NetBIOS name resolution method). The meaning of each node type is as follows:

- b-node: Broadcast node
- p-node: Peer to peer node (WINS only)
- m-node: Mixed node (WINS is used when the IP address is not found by a broadcast)
- h-node: Hybrid node (broadcasting is used when the IP address is not found by WINS)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

network

The "network" command specifies the subnet of the network to which an IP address is dynamically distributed by DHCP. IP addresses whose host name portion is set to all 0s or all 1s are not included in the DHCP address pool.

Syntax

To set or change information:

network <IP Address> [{<Mask> | /<Masklen>}]

To delete information:

no network

Input mode

```
(dhcp-config)
```

Parameters

<IP Address> [{<Mask> | /<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 25-2: IP address range for each class

Class	IP address
Class A (/8)	1.x.x.x to 127.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
   - Addresses that do not belong to class A, B, or C

{<Mask> | /<Masklen>}

1. Default value when this parameter is omitted:
   A mask corresponding to class A, B, or C
2. Range of values:
   For <Mask>, specify a value in the range from 255.0.0.0 to 255.255.255.255.
   For <Masklen>, specify a value in the range from 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. When this command is set, the IP addresses ensured for the DHCP address pool are IP addresses that exclude those where the bits in the host part of the target subnet are all 1s or all 0s. Therefore, use the "ip dhcp excluded-address" command in advance to designate IP addresses that should not be distributed.
2. This command cannot be set together with the "host" and "hardware-address" commands in the same DHCP address pool setting.
3. DHCP address 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).

service dhcp

The "service dhcp" command specifies the interface on which a DHCP server is enabled. Only the interface with this configuration receives DHCP packets.

Syntax

To set information:

service dhcp vlan <vlan id>

To delete information:

no service dhcp vlan <vlan id>

Input mode

```
(config)
```

Parameters

vlan <vlan id>

Specifies 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:

   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

26 Flow Detection Modes/Flow Performance

flow detection mode

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

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

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

Because this command is used to set the basic conditions under which the hardware runs, make sure you set this command during the first stage of actual operation. We recommend that you do not make any changes during operation.

Syntax

To set or change information:

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

To delete information:

no flow detection mode

Input mode

```
(config)
```

Parameters

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

Specifies a flow detection mode for which a hardware table allocation is predefined.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

The following table describes the commands applicable to the flow detection modes.

Table 26-1: Commands applicable to flow detection mode (filter)

Flow detection mode	Applicable command		
	mac access-group	ip access-group	ipv6 traffic-filter
	in/out	in/out	in/out
layer2-1	Y	N	N
layer2-2	N	Y	N
layer2-3	N	Y	Y

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

Table 26-2: Commands applicable to flow detection mode (QoS)

Flow detection mode	Applicable command		
	mac qos-flow-group	ip qos-flow-group	ipv6 qos-flow-group
	in/out	in/out	in/out
layer2-1	Y	N	N
layer2-2	N	Y	N
layer2-3	N	Y	Y

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

For each flow detection mode, see "Configuration Guide Vol. 2, 1.1.3 Flow detection mode" and "Configuration Guide Vol. 2, 3.1.1 Flow detection mode".

Default behavior

The flow detection mode is set to layer 2-1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

27 Access Lists

Names and values that can be specified

■ Protocol names (IPv4)

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

Table 27-1: Protocol names that can be specified (IPv4)

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

■ Protocol names (IPv6)

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

Table 27-2: Protocol names that can be specified (IPv6)

Protocol name	Applicable protocol number
gre	47
icmp	58
ipv6	All IP protocols
ospf	89
pcp	108
pim	103
sctp	132

Protocol name	Applicable protocol number
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 27-3: Port names that can be specified for TCP

Port name	Applicable port name and number
bgp	Border Gateway Protocol version 4 (179)
chargen	Character generator (19)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
exec	Remote process execution (512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (20)
gopher	Gopher (70)
hostname	NIC Host Name Server (101)
http	HyperText Transfer Protocol (80)
https	HTTP over TLS/SSL (443)
ident	Ident Protocol (113)
imap3	Interactive Mail Access Protocol version 3 (220)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)
lpd	Printer service (515)

Port name	Applicable port name and number
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 27-4: Port names that can be specified for UDP (IPv4)

Port name	Applicable port name and number
biff	Biff (512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)

Port name	Applicable port name and number
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 27-5: Port names that can be specified for UDP (IPv6)

Port name	Applicable port name and number
biff	Biff (512)
dhcpv6-client	DHCPv6 client (546)
dhcpv6-server	DHCPv6 server (547)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
ripng	Routing Information Protocol next generation (521)

Port name	Applicable port name and number
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

■ tos names

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

Table 27-6: tos names that can be specified

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

■ precedence names

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

Table 27-7: precedence names that can be specified

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

precedence name	precedence value
priority	1
routine	0

■ DSCP names

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

Table 27-8: DSCP names that can be specified

DSCP name	DSCP value
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
default	0
ef	46

■ Ethernet type name

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

Table 27-9: Ethernet type names that can be specified

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

#: The value is not made public.

■ Destination MAC address names

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

Table 27-10: Destination MAC address names that can be specified

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

#

This applies to IEEE 802.1AB/D6.0 frames only. Specify this with the value to target IEEE Std 802.1AB frames.

■ Message names (ICMP)

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

Table 27-11: 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

Message name	Message	Type	Code
conversion-error	Datagram conversion	31	Not specified
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	Not specified
echo-reply	Echo reply	0	Not specified
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1
information-reply	Information replies	16	Not specified
information-request	Information requests	15	Not specified
mask-reply	Mask replies	18	Not specified
mask-request	Mask requests	17	Not specified
mobile-redirect	Mobile host redirect	32	Not specified
net-redirect	Network redirect	5	0
net-tos-redirect	Network redirect for TOS	5	2
net-tos-unreachable	Network unreachable for TOS	3	11
net-unreachable	Network unreachable	3	0
network-unknown	Network unknown	3	6
no-room-for-option	Parameter required but no room	12	2
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4
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

Message name	Message	Type	Code
redirect	All redirects	5	Not specified
router-advertisement	Router discovery advertisements	9	Not specified
router-solicitation	Router discovery solicitations	10	Not specified
source-quench	Source quenches	4	Not specified
source-route-failed	Source route failed	3	5
time-exceeded	All time exceeded	11	Not specified
timestamp-reply	Timestamp replies	14	Not specified
timestamp-request	Timestamp requests	13	Not specified
traceroute	Traceroute	30	Not specified
ttl-exceeded	TTL exceeded	11	0
unreachable	All unreachable	3	Not specified

Table 27-12: Message names that can be specified for ICMP (IPv6)

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

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

■ Number of access lists that can be created

The number of access lists that can be created is the number of names that can be used as access list IDs.

■ Number of specifications that can be set for an interface

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

Specifications are counted separately for the receiving side and sending side. For example, if an access list is set for both the receiving side and sending side of the same interface, two lists are counted regardless of whether the same access list name is specified.

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

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

Table 27-13: Examples for calculating the number of access lists that can be created and the number of specifications that can be set for an interface

Sample code	Number of access lists that can be created for use	Number of specifications that can be set for an interface

In this example, access list AAA is created and applied to in-bound on Ethernet interface 1/0/1.
`interface gigabitethernet 1/0/1`
`ip access-group AAA in`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 list	1 list

Sample code	Number of access lists that can be created for use	Number of specifications that can be set for an interface

In this example, access list AAA is created and applied to inbound on Ethernet interfaces 1/0/1 and 1/0/2.
`interface gigabitethernet 1/0/1`
`ip access-group AAA in`
 	
`interface gigabitethernet 1/0/2`
`ip access-group AAA in`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 list	2 lists

In this example, access list AAA is created and applied to inbound and outbound on Ethernet interface 1/0/1.
`interface gigabitethernet 1/0/1`
`ip access-group AAA in`
`ip access-group AAA out`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
	1 list	2 lists

In this example, access list AAA is created and applied to inbound on Ethernet interface 1/0/1.
In this example, access list BBB is created and applied to inbound on Ethernet interface 1/0/2.
`interface gigabitethernet 1/0/1`
`ip access-group AAA in`
 	
`interface gigabitethernet 1/0/2`
`ip access-group BBB in`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
 	
`ip access-list extended BBB`
`10 permit udp any any`
`20 deny tcp any any`
	2 lists	2 lists

In this example, access list AAA is created and applied to inbound on Ethernet interface 1/0/1.
In this example, access list BBB is created and applied to outbound on Ethernet interface 1/0/1.
`interface gigabitethernet 1/0/1`
`ip access-group AAA in`
`ip access-group BBB out`
 	
`ip access-list extended AAA`
`10 permit tcp any any`
`20 deny udp any any`
 	
`ip access-list extended BBB`
`10 permit udp any any`
`20 deny tcp any any`
	2 lists	2 lists

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

access-list

Sets an access list used as an IPv4 filter. There are two types of access lists that serve as IPv4 filters. One type is an IPv4 address filter and the other type is an IPv4 packet filter. An IPv4 address filter filters packets based on IPv4 address. An IPv4 packet filter filters based on source IPv4 address, destination IPv4 address, VLAN ID, user priority, ToS field value, port number, TCP flag, ICMP type, and ICMP code.

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

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device.

You can create a maximum of 2048 filter condition entries per IPv4 address filter or IPv4 packet filter.

A maximum of 1024 remark parameters can be specified for access lists and QoS flow lists per device.

For details about access lists, see "■Number of access lists that can be created".

Syntax

To set or change information:

Configuring supplementary information

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

Configuring an IPv4 address filter

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

Configuring an IPv4 packet filter

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

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

filter-condition

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

  {deny | permit} {ip | <protocol>} {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

  {deny | permit} tcp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[eq <source port>] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [eq <destination port>] [ack] [fin] [psh] [rst] [syn] [urg] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is UDP

  {deny | permit} udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[eq <source port>] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [eq <destination port>] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  {deny | permit} icmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is IGMP

  {deny | permit} igmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

To delete information:

no access-list <access list number>

Input mode

```
(config)
```

Parameters

<access list number>

Specifies the identifier used to identify the access list.

This identifier is used to reference the access list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

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

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

remark <remark>

Sets supplementary information for an access list.

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

1. Default value when this parameter is omitted:

   The initial value is null.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

Filter condition parameters

{deny | permit}

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

Specifying deny denies access.

Specifying permit permits access.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

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

Specifies the IPv4 address.

To specify all IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <ipv4>, specify an IPv4 address.

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

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

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

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

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

Specifies the upper layer protocol condition for IPv4 packets.

Note that if all protocols are applicable, specify ip.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details about the protocol names that can be specified, see "Table 27-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard>| host <source ipv4> | any}

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <source ipv4> <source ipv4 wildcard>, host <source ipv4>, or any.

   Specify the source IPv4 address for <source ipv4>.

   For <source ipv4 wildcard>, specify a wildcard mask in IPv4 address format that specifies bits in

an IPv4 address whose permitted value is arbitrary.

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

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

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

eq <source port>

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 27-3: Port names that can be specified for TCP" and "Table 27-4: Port names that can be specified for UDP (IPv4)".

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

{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <destination ipv4> <destination ipv4 wildcard>, host <destination ipv4>, or any.

   Specify the destination IPv4 address for <destination ipv4>.

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

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

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

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

eq <destination port>

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.

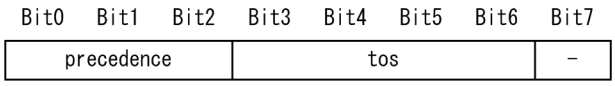
   For details about the port names that can be specified, see "Table 27-3: Port names that can be specified for TCP" and "Table 27-4: Port names that can be specified for UDP (IPv4)".

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

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:

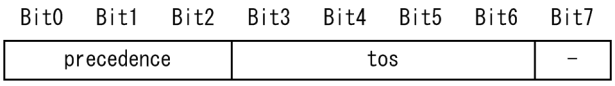
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see "Table 27-6: tos names that can be specified".

precedence <precedence>

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

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



1. Default value when this parameter is omitted:

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

2. Range of values:

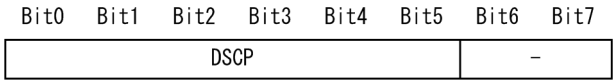
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see "Table 27-7: precedence names that can be specified".

dscp <dscp>

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

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



1. Default value when this parameter is omitted:

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

2. Range of values:

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

   For details about the DSCP names that can be specified, see "Table 27-8: 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 27-11: Message names that can be specified for ICMP (IPv4)".

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

vlan <vlan id>

Specifies a VLAN ID.

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   See "Specifiable values for parameters".

user-priority <priority>

Specifies the user priority.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify 0 to 7 in decimal.

Default behavior

None

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. In IPv4 address filtering, if you omit the address mask when specifying the target IP host address, 0.0.0.0 is used as the mask.
2. For <access list number>, you can use 1 to 99 or 1300 to 1999 in the "ip access-list standard" command.
3. For <access list number>, you can use 100 to 199 or 2000 to 2699 in the "ip access-list extended" command.
4. When 255.255.255.255 is entered for an IPv4 address wildcard mask, a source address wildcard mask, or a destination address wildcard mask, any is displayed.
5. If nnn.nnn.nnn.nnn 0.0.0.0 is entered as the IPv4 address, the source address, and the destination address, host nnn.nnn.nnn.nnn is displayed.
6. The protocol name ah and the protocol number 51 (in decimal) cannot be set in <protocol> as detection conditions for filtering.

deny (ip access-list extended)

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

Syntax

To set or change information:

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

  [<sequence>] deny {ip | <protocol>} {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

- When the upper layer protocol is TCP

  [<sequence>] deny tcp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[eq <source port>] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [eq <destination port>] [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

  [<sequence>] deny udp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}[eq <source port>] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [eq <destination port>] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

- When the upper layer protocol is ICMP

  [<sequence>] deny icmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

- When the upper layer protocol is IGMP

  [<sequence>] deny igmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

To delete information:

no <sequence>

Input mode

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

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

   Note, however, that if the maximum value for the application sequence is greater than 4294967284,

the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the upper layer protocol condition for IPv4 packets.

Note that if all protocols are applicable, specify ip.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details about the protocol names that can be specified, see "Table 27-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <source ipv4> <source ipv4 wildcard>, host <source ipv4>, or any.

   Specify the source IPv4 address for <source ipv4>.

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

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

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

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

eq <source port>

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 27-3: Port names that can be specified for TCP" and "Table 27-4: Port names that can be specified for UDP (IPv4)".

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

{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

Specify <destination ipv4> <destination ipv4 wildcard>, host <destination ipv4>, or any.

Specify the destination IPv4 address for <destination ipv4>.

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

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

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

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

eq <destination port>

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.

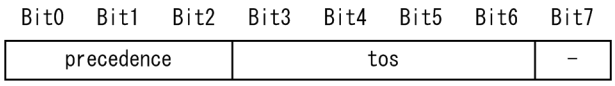
   For details about the port names that can be specified, see "Table 27-3: Port names that can be specified for TCP" and "Table 27-4: Port names that can be specified for UDP (IPv4)".

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

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:

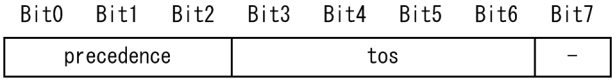
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see "Table 27-6: tos names that can be specified".

precedence <precedence>

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

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



1. Default value when this parameter is omitted:

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

2. Range of values:

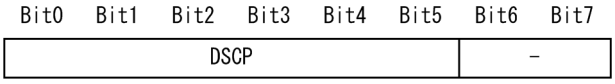
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see "Table 27-7: precedence names that can be specified".

dscp <dscp>

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

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



1. Default value when this parameter is omitted:

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

2. Range of values:

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

   For details about the DSCP names that can be specified, see "Table 27-8: 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 27-11: 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>]

This parameter is an option for using the dynamic ACL/QoS.

Specify the user class and class mask.

For <class mask>, specify the class mask that sets the bits to be compared in <class>. If <class mask> is omitted, all bits will be 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. When 255.255.255.255 is entered for the source address wildcard mask and the destination address wildcard mask, any is displayed.
2. If nnn.nnn.nnn.nnn 0.0.0.0 is entered as the source address and the destination address, host nnn.nnn.nnn.nnn is displayed.
3. The protocol name ah and the protocol number 51 (in decimal) cannot be set in <protocol> as detection conditions for filtering.

deny (ip access-list standard)

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

Syntax

To set or change information:

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

To delete information:

no <sequence>

Input mode

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

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the IPv4 address.

To specify all IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <ipv4>, specify an IPv4 address.

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

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

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

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

Default behavior

None

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

deny (ipv6 access-list)

Specifies the conditions by which the IPv6 filter denies access.

Syntax

To set or change information:

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

  [<sequence>] deny {ipv6 | <protocol>} {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

  [<sequence>] deny tcp {<source ipv6>/<length> | host <source ipv6> | any} [eq <source port>] {<destination ipv6>/<length> | host <destination ipv6> | any} [eq <destination port>] [ack] [fin] [psh] [rst] [syn] [urg] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is UDP

  [<sequence>] deny udp {<source ipv6>/<length> | host <source ipv6> | any} [eq <source port>] {<destination ipv6>/<length> | host <destination ipv6> | any} [eq <destination port>] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  [<sequence>] deny icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

To delete information:

no <sequence>

Input mode

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

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the upper layer protocol condition for IPv6 packets.

Note that if all protocols are applicable, specify ipv6.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

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

For details about the protocol names that can be specified, see "Table 27-2: Protocol names that can be specified (IPv6)".

{<source ipv6>/<length> | host <source ipv6> | any}

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify any.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify <source ipv6>/<length>, host <source ipv6>, or any.

Specify the source IPv6 address for <source ipv6>.

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

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

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

<source ipv6> (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):

0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>: 0 to 128

eq <source port>

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 27-3: Port names that can be specified for TCP" and "Table 27-5: Port names that can be specified for UDP (IPv6)".

The filter condition is an exact match of <source port>.

{<destination ipv6>/<length> | host <destination ipv6> | any}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify any.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify <destination ipv6>/<length>, host <destination ipv6>, or any.

Specify the destination IPv6 address for <destination ipv6>.

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

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

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

<destination ipv6> (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):

0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>: 0 to 128

eq <destination port>

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 27-3: Port names that can be specified for TCP" and "Table 27-5: Port names that can be specified for UDP (IPv6)".

   The filter condition is an exact match of <destination port>.

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.)

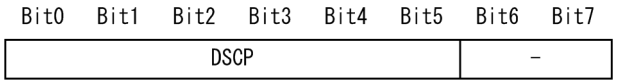
2. Range of values:

   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 27-8: 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 27-12: Message names that can be specified for ICMP (IPv6)".

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

vlan <vlan id>

Specifies a VLAN ID.

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   See "Specifiable values for parameters".

user-priority <priority>

Specifies the user priority.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify 0 to 7 in decimal.

Default behavior

None

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/0 is entered as the source address and the destination address, any is displayed.
2. If nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/128 is entered as the source address and the destination address, host nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn is displayed.

deny (mac access-list extended)

Specifies the conditions by which the MAC filter denies access.

Syntax

To set or change information:

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

To delete information:

no <sequence>

Input mode

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

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the source MAC address.

To specify all source MAC addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   Specify the source MAC address for <source mac>.

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

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

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

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

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

Specifies the destination MAC address.

To specify all destination MAC addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   Specify the destination MAC address for <destination mac>.

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

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

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

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

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

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

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

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

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

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

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

<ethernet type>

Specifies the Ethernet type number.

1. Default value when this parameter is omitted:

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

2. Range of values:

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

   For details about the Ethernet type names that can be specified, see "Table 27-9: 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>]

This parameter is an option for using the dynamic ACL/QoS.

Specify the user class and class mask.

For <class mask>, specify the class mask that sets the bits to be compared in <class>. If <class mask> is omitted, all bits will be 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 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 27-10: 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.

ip access-group

Applies an IPv4 access list to an Ethernet interface or a VLAN interface, and enables the IPv4 filter function. A maximum of 540 lists of ip access-group, ipv6 traffic-filter, and mac access-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

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

To delete information:

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

Input mode

```
(config-if)
```

Ethernet interface, VLAN interface

Parameters

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <access list name>, specify a name that is no more than 31 characters.

   For details, see "Specifiable values for parameters".

{in | out}

Specifies whether the filter is Inbound or Outbound.

in: Inbound for the filter (Specifies the receiving side)

out: Outbound for the filter (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. If you specify a non-existent IPv4 filter, this will be ignored. The identifier of the IPv4 filter is registered.
2. 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.
3. 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.
4. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if no tunneling ports have been set for the Ethernet interface for the device.
5. An access list can be set on the sending side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the device.
6. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if tag translation has not been set for the target interface.
7. You can set an access list on the sending side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.

ip access-list extended

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

This command sets an IPv4 packet filter.

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

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device.

You can create a maximum of 2048 filter condition entries per IPv4 address filter or IPv4 packet filter.

For details about access lists, see "■Number of access lists that can be created".

Syntax

To set information:

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

To delete information:

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

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <access list name>, specify a name that is no more than 31 characters.

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

ip access-list resequence

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

Syntax

To set or change information:

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

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <access list name>, specify a name that is no more than 31 characters.

   For details, see "Specifiable values for parameters".

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip access-list standard

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

This command sets an IPv4 address filter.

An IPv4 address filter filters packets based on IPv4 address.

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device.

You can create a maximum of 2048 filter condition entries per IPv4 address filter or IPv4 packet filter.

For details about access lists, see "■Number of access lists that can be created".

Syntax

To set information:

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

To delete information:

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

Input mode

```
(config)
```

Parameters

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

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <access list name>, specify a name that is no more than 31 characters.

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

ipv6 access-list

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

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 filter condition entries can be created.

For details about access lists, see "■Number of access lists that can be created".

Syntax

To set information:

ipv6 access-list <access list name>

To delete information:

no ipv6 access-list <access list name>

Input mode

```
(config)
```

Parameters

<access list name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

ipv6 access-list resequence

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

Syntax

To set or change information:

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

Input mode

```
(config)
```

Parameters

<access list name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details, see "Specifiable values for parameters".

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ipv6 traffic-filter

Applies an IPv6 access list to an Ethernet interface or a VLAN interface, and enables the IPv6 filter function.

A maximum of 540 lists of ip access-group, ipv6 traffic-filter, and mac access-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

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

To delete information:

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

Input mode

```
(config-if)
```

Ethernet interface, VLAN interface

Parameters

<access list name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details, see "Specifiable values for parameters".

{in | out}

Specify whether the filter is Inbound or Outbound.

in: Inbound for the filter (Specifies the receiving side)

out: Outbound for the filter (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 filters on the same interface. If a filter has already been set, first remove it and then set it again.
2. If you specify a non-existent IPv6 filter, this will be ignored. The identifier of the IPv6 filter is registered.
3. If a VLAN parameters is included as a flow detection condition, the flow detection mode can be set if the VLAN ID is included in the Ethernet interface settings to be applied.
4. When IPv6 packet filtering is applied to a VLAN interface, the flow detection mode can be set if no VLAN parameters are included as a flow detection condition.
5. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if no tunneling ports have been set for the Ethernet interface for the device.
6. An access list can be set on the sending side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the device.
7. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if tag translation has not been set for the target interface.
8. You can set an access list on the sending side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.

mac access-group

Applies a MAC access list to an Ethernet interface or a VLAN interface and enables the MAC filter function. A maximum of 540 lists of ip access-group, ipv6 traffic-filter, and mac access-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

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

To delete information:

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

Input mode

```
(config-if)
```

Ethernet interface, VLAN interface

Parameters

<access list name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details, see "Specifiable values for parameters".

{in | out}

Specifies whether the filter is Inbound or Outbound.

in: Inbound for the filter (Specifies the receiving side)

out: Outbound for the filter (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. If you specify a non-existent MAC filter, this will be ignored. The identifier of a MAC access list is registered.
2. 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.
3. 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.
4. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if no tunneling ports have been set for the Ethernet interface for the device.
5. An access list can be set on the sending side of the VLAN interface if no tunneling ports have been set for the Ethernet interface for the device.
6. An access list that contains a VLAN parameter as a flow detection condition can be set on the sending side if tag translation has not been set for the target interface.
7. You can set an access list on the sending side of a VLAN interface if tag translation has not been set for the Ethernet interface contained in the VLAN interface.

mac access-list extended

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

A maximum of 1024 access lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 filter condition entries can be created.

For details about access lists, see "■Number of access lists that can be created".

Syntax

To set information:

mac access-list extended <access list name>

To delete information:

no mac access-list extended <access list name>

Input mode

```
(config)
```

Parameters

<access list name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

mac access-list resequence

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

Syntax

To set or change information:

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

Input mode

```
(config)
```

Parameters

<access list name>

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

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details, see "Specifiable values for parameters".

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 (in decimal).

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

permit (ip access-list extended)

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

Syntax

To set or change information:

[<sequence>] permit {<filter-condition>}

filter-condition

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

  {ip | <protocol>} {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [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>] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [eq <destination port>] [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>] {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [eq <destination port>] [{[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>]]

- When the upper layer protocol is IGMP

  igmp {<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any} {<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any} [{[tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

To delete information:

no <sequence>

Input mode

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

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

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

2. Range of values:

Specify 1 to 4294967294 in decimal.

Filter condition parameters

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

Specifies the upper layer protocol condition for IPv4 packets.

Note that if all protocols are applicable, specify ip.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

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

For details about the protocol names that can be specified, see "Table 27-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

This parameter cannot be omitted.

2. Range of values:

Specify <source ipv4> <source ipv4 wildcard>, host <source ipv4>, or any.

Specify the source IPv4 address for <source ipv4>.

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

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

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

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

eq <source port>

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 27-3: Port names that can be specified for TCP" and "Table 27-4: Port names that can be specified for UDP (IPv4)".

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

{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <destination ipv4> <destination ipv4 wildcard>, host <destination ipv4>, or any.

   Specify the destination IPv4 address for <destination ipv4>.

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

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

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

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

eq <destination port>

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.

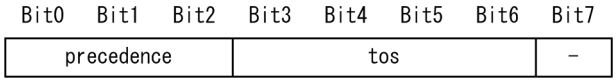
   For details about the port names that can be specified, see "Table 27-3: Port names that can be specified for TCP" and "Table 27-4: Port names that can be specified for UDP (IPv4)".

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

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:

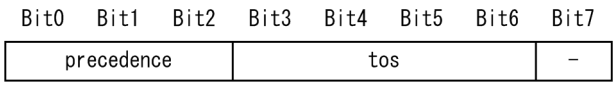
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see "Table 27-6: tos names that can be specified".

precedence <precedence>

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

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



1. Default value when this parameter is omitted:

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

2. Range of values:

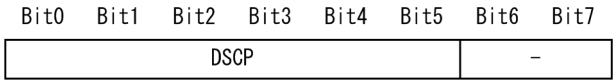
Specify 0 to 7 (in decimal) or the precedence name.

For details about the precedence names that can be specified, see "Table 27-7: precedence names that can be specified".

dscp <dscp>

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

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



1. Default value when this parameter is omitted:

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

2. Range of values:

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

   For details about the DSCP names that can be specified, see "Table 27-8: 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 27-11: 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>]

This parameter is an option for using the dynamic ACL/QoS.

Specify the user class and class mask.

For <class mask>, specify the class mask that sets the bits to be compared in <class>. If <class mask> is omitted, all bits will be 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. When 255.255.255.255 is entered for the source address wildcard mask and the destination address wildcard mask, any is displayed.
2. If nnn.nnn.nnn.nnn 0.0.0.0 is entered as the source address and the destination address, host nnn.nnn.nnn.nnn is displayed.

permit (ip access-list standard)

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

Syntax

To set or change information:

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

To delete information:

no <sequence>

Input mode

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

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

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

Specifies the IPv4 address.

To specify all IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For <ipv4>, specify an IPv4 address.

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

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

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

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

Default behavior

None

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

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

permit (ipv6 access-list)

Specifies the conditions by which the IPv6 filter permits access.

Syntax

To set or change information:

[<sequence>] permit {<filter-condition>}

filter-condition

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

  {ipv6 | <protocol>} {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is TCP

  tcp {<source ipv6>/<length> | host <source ipv6> | any} [eq <source port>] {<destination ipv6>/<length> | host <destination ipv6> | any} [eq <destination port>] [ack] [fin] [psh] [rst] [syn] [urg] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is UDP

  udp {<source ipv6>/<length> | host <source ipv6> | any} [eq <source port>] {<destination ipv6>/<length> | host <destination ipv6> | any} [eq <destination port>] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- When the upper layer protocol is ICMP

  icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length>| host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [{<icmp type> [<icmp code>] | <icmp message>}] [vlan <vlan id>] [user-priority <priority>]

To delete information:

no <sequence>

Input mode

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

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

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

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

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

2. Range of values:

   Specify 1 to 4294967294 in decimal.

Filter condition parameters

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

Specifies the upper layer protocol condition for IPv6 packets.

Note that if all protocols are applicable, specify ipv6.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

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

   For details about the protocol names that can be specified, see "Table 27-2: Protocol names that can be specified (IPv6)".

{<source ipv6>/<length> | host <source ipv6> | any}

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <source ipv6>/<length>, host <source ipv6>, or any.

   Specify the source IPv6 address for <source ipv6>.

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

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

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

   <source ipv6> (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):

   0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <length>: 0 to 128

eq <source port>

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 27-3: Port names that can be specified for TCP" and "Table 27-5: Port names that can be specified for UDP (IPv6)".

   The filter condition is an exact match of <source port>.

{<destination ipv6>/<length> | host <destination ipv6> | any}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <destination ipv6>/<length>, host <destination ipv6>, or any.

   Specify the destination IPv6 address for <destination ipv6>.

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

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

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

<destination ipv6> (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):

0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>: 0 to 128

eq <destination port>

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 27-3: Port names that can be specified for TCP" and "Table 27-5: Port names that can be specified for UDP (IPv6)".

   The filter condition is an exact match of <destination port>.

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.)

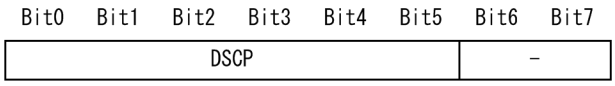
2. Range of values:

   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 27-8: 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 27-12: Message names that can be specified for ICMP (IPv6)".

1. Default value when this parameter is omitted:

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

2. Range of values:

   None

vlan <vlan id>

Specifies a VLAN ID.

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

1. Default value when this parameter is omitted:

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

2. Range of values:

   See "Specifiable values for parameters".

user-priority <priority>

Specifies the user priority.

1. Default value when this parameter is omitted:

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

2. Range of values:

   Specify 0 to 7 in decimal.

Default behavior

None

Impact on communication

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

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/0 is entered as the source address and the destination address, any is displayed.
2. If nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/128 is entered as the source address and the destination address, host nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn is displayed.

permit (mac access-list extended)

Specifies the conditions by which the MAC filter permits access.

Syntax

To set or change information:

[<sequence>] permit {<filter-condition>}

filter-condition

{<source mac> <source mac mask> | host <source mac> | any} {<destination mac> <destination mac mask> | host <destination mac> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol } [<ethernet type>] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

To delete information:

no <sequence>

Input mode

```
(config-ext-macl)
```

Parameters

<sequence>

Specifies the sequence in which filter conditions are applied.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the access list.

   If conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

   Note, however, that if the maximum value for the application sequence is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

Filter condition parameters

{<source mac> <source mac mask> | host <source mac> | any}

Specifies the source MAC address.

To specify all source MAC addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <source mac> <source mac mask>, host <source mac>, or any.

   Specify the source MAC address for <source mac>.

   For <source mac mask>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   If host <source mac> is specified, the filter condition is an exact match of <source mac>.

If any is specified, the source MAC address is not used as a filter condition.

MAC address (nnnn.nnnn.nnnn): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{<destination mac> <destination mac mask> | host <destination mac> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol }

Specifies the destination MAC address.

To specify all destination MAC addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <destination mac> <destination mac mask>, host <destination mac>, any, bpdu, cdp, lacp, lldp, oadp, pvst-plus-bpdu, or slow-protocol.

   Specify the destination MAC address for <destination mac>.

   For <destination mac mask>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   If host <destination mac> is specified, the filter condition is an exact match of <destination mac>.

   If bpdu is specified, BPDU control packets are used as the filter condition.

   If cdp is specified, CDP control packets are used as the filter condition.

   If lacp or slow-protocol is specified, slow protocol packets are used as the filter condition.

   This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD function.

   If lldp is specified, LLDP control packets are used as the filter condition.

   If oadp is specified, OADP control packets are used as the filter condition.

   If pvst-plus-bpdu is specified, PVST+ control packets are used as the filter condition.

   MAC address (nnnn.nnnn.nnnn): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<ethernet type>

Specifies the Ethernet type number.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name.

   For details about the Ethernet type names that can be specified, see "Table 27-9: 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>]

This parameter is an option for using the dynamic ACL/QoS.

Specify the user class and class mask.

For <class mask>, specify the class mask that sets the bits to be compared in <class>. If <class mask> is omitted, all bits will be 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 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 27-10: 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.

remark

Specifies supplementary information for the access list. Access lists are available for IPv4 address filtering, IPv4 packet filtering, IPv6 filtering, and MAC filtering. A maximum of 1024 information items can be specified for access lists and QoS flow lists per device.

Syntax

To set or change information:

remark <remark>

To delete information:

no remark

Input mode

```
(config-ext-nacl)
(config-std-nacl)
(config-ipv6-acl)
(config-ext-macl)
```

Parameters

<remark>

Sets supplementary information for the target access list according to input mode.

One line can be set for each access list. Entering new information overwrites the existing information.

1. Default value when this parameter is omitted:

   The initial value is null.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

28 QoS

Names and values that can be specified

■ Protocol names (IPv4)

The following table lists the names that can be specified as IPv4 protocol names.

Table 28-1: Protocol names that can be specified (IPv4)

Protocol name	Applicable protocol number
ah#	51#
esp	50
gre	47
icmp	1
igmp	2
ip	All IP protocols
ipinip	4
ospf	89
pcp	108
pim	103
sctp	132
tcp	6
tunnel	41
udp	17
vrrp	112

#: The protocol name ah and the protocol number 51 cannot be detected as flow conditions.

■ Protocol names (IPv6)

The following table lists the names that can be specified as IPv6 protocol names.

Table 28-2: Protocol names that can be specified (IPv6)

Protocol name	Applicable protocol number
gre	47
icmp	58
ipv6	All IP protocols
ospf	89
pcp	108
pim	103

Protocol name	Applicable protocol number
sctp	132
tcp	6
tunnel	4
udp	17
vrrp	112

■ Port names (TCP)

The following table lists the port names that can be specified for TCP.

Table 28-3: Port names that can be specified for TCP

Port name	Applicable port name and number
bgp	Border Gateway Protocol version 4 (179)
chargen	Character generator (19)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
exec	Remote process execution (512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (20)
gopher	Gopher (70)
hostname	NIC Host Name Server (101)
http	HyperText Transfer Protocol (80)
https	HTTP over TLS/SSL (443)
ident	Ident Protocol (113)
imap3	Interactive Mail Access Protocol version 3 (220)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
ldap	Lightweight Directory Access Protocol (389)
login	Remote login (513)

Port name	Applicable port name and number
lpd	Printer service (515)
nntp	Network News Transfer Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
pop3s	POP3 over TLS/SSL (995)
raw	Printer PDL Data Stream (9100)
shell	Remote commands (514)
smtp	Simple Mail Transfer Protocol (25)
smtps	SMTP over TLS/SSL (465)
ssh	Secure Shell Remote Login Protocol (22)
sunrpc	Sun Remote Procedure Call (111)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nicname (43)

■ Port names (UDP)

The following table lists the port names that can be specified for UDP.

Table 28-4: Port names that can be specified for UDP (IPv4)

Port name	Applicable port name and number
biff	Biff (512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)

Port name	Applicable port name and number
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

Table 28-5: Port names that can be specified for UDP (IPv6)

Port name	Applicable port name and number
biff	Biff (512)
dhcpv6-client	DHCPv6 client (546)
dhcpv6-server	DHCPv6 server (547)
discard	Discard (9)
domain	Domain Name System (53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (500)
mobile-ip	Mobile IP registration (434)
nameserver	Host Name Server (42)
ntp	Network Time Protocol (123)
radius	Remote Authentication Dial In User Service (1812)
radius-acct	RADIUS Accounting (1813)

Port name	Applicable port name and number
ripng	Routing Information Protocol next generation (521)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs+	Terminal Access Controller Access Control System Plus (49)
tacacs-ds	TACACS-Database Service (65)
talk	like tenex link (517)
tftp	Trivial File Transfer Protocol (69)
time	Time server protocol (37)
who	Who service (513)
xdmcp	X Display Manager Control Protocol (177)

■ tos names

The following table lists the tos names that can be specified.

Table 28-6: tos names that can be specified

tos name	tos value
max-reliability	2
max-throughput	4
min-delay	8
min-monetary-cost	1
normal	0

■ precedence names

The following table lists the precedence names that can be specified.

Table 28-7: precedence names that can be specified

precedence name	precedence value
critical	5
flash	3
flash-override	4
immediate	2
internet	6

precedence name	precedence value
network	7
priority	1
routine	0

■ DSCP names

The following table lists the DSCP names that can be specified.

Table 28-8: DSCP names that can be specified

DSCP name	DSCP value
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
default	0
ef	46

■ Ethernet type name

The following table lists the Ethernet type names that can be specified.

Table 28-9: Ethernet type names that can be specified

Ethernet type name	Ethernet value	Remarks
appletalk	0x809b	
arp	0x0806	
axp	0x88f3	Alaxala Protocol
eapol	0x888e	
gsrp	__#	Performs flow detection for GSRP control packets.
ipv4	0x0800	
ipv6	0x86dd	
ipx	0x8137	
xns	0x0600	

#: The value is not made public.

■ Destination MAC address names

The following table lists the destination MAC address names that can be specified.

Table 28-10: Destination MAC address names that can be specified

Destination address specification	Destination address	Destination address mask
bpdu	0180.C200.0000	0000.0000.0000
cdp	0100.0CCC.CCCC	0000.0000.0000
lacp	0180.C200.0002	0000.0000.0000
lldp	0100.8758.1310#	0000.0000.0000
oadp	0100.4C79.FD1B	0000.0000.0000
pvst-plus-bpdu	0100.0CCC.CCCD	0000.0000.0000
slow-protocol	0180.C200.0002	0000.0000.0000

#:

This applies to IEEE 802.1AB/D6.0 frames only. Specify this with the value to target IEEE Std 802.1AB frames.

■ Message names (ICMP)

The following table lists the message names that can be specified for ICMP.

Table 28-11: 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

Message name	Message	Type	Code
conversion-error	Datagram conversion	31	Not specified
dod-host-prohibited	Host prohibited	3	10
dod-net-prohibited	Network prohibited	3	9
echo	Echo (ping)	8	Not specified
echo-reply	Echo reply	0	Not specified
general-parameter-problem	Parameter problem	12	0
host-isolated	Host isolated	3	8
host-precedence-unreachable	Host unreachable for precedence	3	14
host-redirect	Host redirect	5	1
host-tos-redirect	Host redirect for TOS	5	3
host-tos-unreachable	Host unreachable for TOS	3	12
host-unknown	Host unknown	3	7
host-unreachable	Host unreachable	3	1
information-reply	Information replies	16	Not specified
information-request	Information requests	15	Not specified
mask-reply	Mask replies	18	Not specified
mask-request	Mask requests	17	Not specified
mobile-redirect	Mobile host redirect	32	Not specified
net-redirect	Network redirect	5	0
net-tos-redirect	Network redirect for TOS	5	2
net-tos-unreachable	Network unreachable for TOS	3	11
net-unreachable	Network unreachable	3	0
network-unknown	Network unknown	3	6
no-room-for-option	Parameter required but no room	12	2
option-missing	Parameter required but not present	12	1
packet-too-big	Fragmentation needed and DF set	3	4
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

Message name	Message	Type	Code
redirect	All redirects	5	Not specified
router-advertisement	Router discovery advertisements	9	Not specified
router-solicitation	Router discovery solicitations	10	Not specified
source-quench	Source quenches	4	Not specified
source-route-failed	Source route failed	3	5
time-exceeded	All time exceeded	11	Not specified
timestamp-reply	Timestamp replies	14	Not specified
timestamp-request	Timestamp requests	13	Not specified
traceroute	Traceroute	30	Not specified
ttl-exceeded	TTL exceeded	11	0
unreachable	All unreachable	3	Not specified

Table 28-12: Message names that can be specified for ICMP (IPv6)

Message name	Message	Type	Code
beyond-scope	Destination beyond scope	1	2
destination-unreachable	Destination address is unreachable	1	3
echo-reply	Echo reply	129	Not specified
echo-request	Echo request (ping)	128	Not specified
header	Parameter header problems	4	0
hop-limit	Hop limit exceeded in transit	3	0
mld-query	Multicast Listener Discovery Query	130	Not specified
mld-reduction	Multicast Listener Discovery Reduction	132	Not specified
mld-report	Multicast Listener Discovery Report	131	Not specified
nd-na	Neighbor discovery neighbor advertisements	136	Not specified
nd-ns	Neighbor discovery neighbor solicitations	135	Not specified
next-header	Parameter next header problems	4	1
no-admin	Administration prohibited destination	1	1
no-route	No route to destination	1	0
packet-too-big	Packet too big	2	Not specified
parameter-option	Parameter option problems	4	2
parameter-problem	All parameter problems	4	Not specified
port-unreachable	Port unreachable	1	4

Message name	Message	Type	Code
reassembly-timeout	Reassembly timeout	3	1
renum-command	Router renumbering command	138	0
renum-result	Router renumbering result	138	1
renum-seq-number	Router renumbering sequence number reset	138	255
router-advertisement	Neighbor discovery router advertisements	134	Not specified
router-renumbering	All router renumbering	138	Not specified
router-solicitation	Neighbor discovery router solicitations	133	Not specified
time-exceeded	All time exceeded	3	Not specified
unreachable	All unreachable	1	Not specified

■ Number of QoS flow lists that can be created

The number of QoS flow lists that can be created is the number of names that can be used as QoS flow list IDs.

■ Number of specifications that can be set for an interface

The number of specifications that can be set for an interface is the total number of QoS flow lists that can be set for an interface.

■ Examples of calculating the number of QoS flow lists that can be created and the number of specifications that can be set for an interface

The following table provides examples of calculating the number of QoS flow lists that can be created and the number of specifications that can be set for an interface.

Table 28-13: Examples for calculating the number of QoS flow lists that can be created and the number of specifications that can be set for an interface

Sample code	Number of QoS flow lists that can be created for use	Number of specifications that can be set for an interface

In this example, QoS flow list AAA is created and applied to inbound on Ethernet interface 1/0/1.
`interface gigabitethernet 1/0/1`
`  ip qos-flow-group AAA in`
 	
`ip qos-flow-list AAA`
`  10 qos tcp any any action replace-user-priority 0`
`  20 qos udp any any action replace-dscp 0`
	1 list	1 list

In this example, QoS flow list AAA is created and applied inbound on Ethernet interfaces 1/0/1 and 1/0/2.
`interface gigabitethernet 1/0/1`
`  ip qos-flow-group AAA in`
 	
`interface gigabitethernet 1/0/2`
`  ip qos-flow-group AAA in`
 	
`ip qos-flow-list AAA`
`  10 qos tcp any any action replace-user-priority 0`
`  20 qos udp any any action replace-dscp 0`
	1 list	2 lists

Sample code	Number of QoS flow lists that can be created for use	Number of specifications that can be set for an interface

In this example, QoS flow list AAA is created and applied to inbound on Ethernet interface 1/0/1.
In this example, QoS flow list BBB is created and applied to inbound on Ethernet interface 1/0/2.
`interface gigabitethernet 1/0/1`
`ip qos-flow-group AAA in`
`interface gigabitethernet 1/0/2`
`ip qos-flow-group BBB in`
`ip qos-flow-list AAA`
`10 qos tcp any any action replace-user-priority 0`
`20 qos udp any any action replace-dscp 0`
`ip qos-flow-list BBB`
`10 qos udp any any action replace-user-priority 0`
`20 qos tcp any any action replace-dscp 0`
	2 lists	2 lists

In this example, QoS flow list AAA is created but not applied to any interface.
`ip qos-flow-list AAA`
`10 qos tcp any any action replace-user-priority 0`
	1 list	0 list

ip qos-flow-group

Enables the QoS function by applying an IPv4 QoS flow list to an Ethernet interface or a VLAN interface. A maximum of 540 lists of ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

ip qos-flow-group <qos flow list name> in

To delete information:

no ip qos-flow-group <qos flow list name> in

Input mode

```
(config-if)
```

Ethernet interface, VLAN interface

Parameters

<qos flow list name>

Specifies the IPv4 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

in

Specifies Inbound.

in: Inbound (Specifies the receiving side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can apply one IPv4 QoS flow list to the inbound side of an interface.
2. If you specify a non-existent IPv4 QoS flow list name, this will be ignored. The IPv4 QoS flow list name is registered.
3. If another list has been set for an interface by using this command, no more lists can be set. Remove the existing list first, and then set another list.
4. 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.

ip qos-flow-list

Creates an IPv4 QoS flow list to be used to set QoS flow detection and action specifications. A maximum of 1024 QoS flow lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 flow detection and action specification entries can be created.

For details about the QoS flow lists, see "■Number of QoS flow lists that can be created".

Syntax

To set information:

ip qos-flow-list <qos flow list name>

To delete information:

no ip qos-flow-list <qos flow list name>

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the IPv4 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify the name of an IPv6 QoS flow list or MAC QoS flow list that has already been created.

ip qos-flow-list resequence

Resets the sequence numbers of the application sequence in the IPv4 QoS flow list.

Syntax

To set or change information:

ip qos-flow-list resequence <qos flow list name> [<starting sequence> [<increment sequence>]]

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the name of the IPv4 QoS flow list to be changed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ipv6 qos-flow-group

Enables the QoS function by applying an IPv6 QoS flow list to an Ethernet interface or a VLAN interface.

A maximum of 540 lists of ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

ipv6 qos-flow-group <qos flow list name> in

To delete information:

no ipv6 qos-flow-group <qos flow list name> in

Input mode

```
(config-if)
```

Ethernet interface, VLAN interface

Parameters

<qos flow list name>

Specifies the IPv6 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

in

Specifies Inbound.

in: Inbound (Specifies the receiving side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can apply one IPv6 QoS flow list to the inbound side of an interface.
2. If you specify a non-existent IPv6 QoS flow list name, this will be ignored. The IPv6 QoS flow list name is registered.
3. If another list has been set for an interface by using this command, no more lists can be set. Remove the existing list first, and then set another list.
4. 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.

ipv6 qos-flow-list

Creates an IPv6 QoS flow list to be used to set QoS flow detection and action specifications. A maximum of 1024 QoS flow lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 flow detection and action specification entries can be created.

For details about the QoS flow lists, see "■Number of QoS flow lists that can be created".

Syntax

To set information:

ipv6 qos-flow-list <qos flow list name>

To delete information:

no ipv6 qos-flow-list <qos flow list name>

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the IPv6 QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify the name of an IPv4 QoS flow list or MAC QoS flow list that has already been created.

ipv6 qos-flow-list resequence

Resets the sequence numbers of the application sequence in the IPv6 QoS flow list.

Syntax

To set or change information:

ipv6 qos-flow-list resequence <qos flow list name> [<starting sequence> [<increment sequence>]]

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the name of the IPv6 QoS flow list to be changed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

mac qos-flow-group

Enables the QoS function by applying a MAC QoS flow list to an Ethernet interface or a VLAN interface. A maximum of 540 lists of ip qos-flow-group, ipv6 qos-flow-group, and mac qos-flow-group can be set for interfaces per device.

For the number of specifications for the interface, see "■Number of specifications that can be set for an interface".

Syntax

To set information:

mac qos-flow-group <qos flow list name> in

To delete information:

no mac qos-flow-group <qos flow list name> in

Input mode

```
(config-if)
```

Ethernet interface, VLAN interface

Parameters

<qos flow list name>

Specifies the MAC QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

in

Specifies Inbound.

in: Inbound (Specifies the receiving side)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can apply one MAC QoS flow list to the inbound side of an interface.
2. If a non-existent MAC QoS flow list name is set, this will be ignored. The MAC QoS flow list name is registered.
3. If another list has been set for an interface by using this command, no more lists can be set. Remove the existing list first, and then set another list.
4. 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.

mac qos-flow-list

Creates a MAC QoS flow list used to set QoS flow detection and action specifications. A maximum of 1024 QoS flow lists (for IPv4, IPv6, and MAC) can be created per device. A maximum of 2048 flow detection and action specification entries can be created.

For details about the QoS flow lists, see "■Number of QoS flow lists that can be created".

Syntax

To set information:

mac qos-flow-list <qos flow list name>

To delete information:

no mac qos-flow-list <qos flow list name>

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the MAC QoS flow list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You cannot specify the name of an IPv4 QoS flow list or IPv6 QoS flow list that has already been created.

mac qos-flow-list resequence

Resets the sequence numbers of the application sequence in the MAC QoS flow list.

Syntax

To set or change information:

mac qos-flow-list resequence <qos flow list name> [<starting sequence> [<increment sequence>]]

Input mode

```
(config)
```

Parameters

<qos flow list name>

Specifies the MAC QoS flow list name to be changed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

<starting sequence>

Specifies the starting sequence number.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

<increment sequence>

Specifies the increment value for the sequence.

1. Default value when this parameter is omitted:

   The initial value is 10.

2. Range of values:

   Specify 1 to 100 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

qos (ip qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv4 QoS flow list.

Syntax

To set or change information:

[<sequence>] qos {flow detection condition} [action specification]

- Flow detection conditions

When the upper layer protocol is other than TCP, UDP, ICMP, and IGMP

{ip | <protocol> }{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [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>]{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[eq <destination port>][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>]{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[eq <destination port>][{ [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>]]

When the upper layer protocol is IGMP

igmp{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any}{<destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any}[{ [tos <tos>] [precedence <precedence>] | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

- Action specification

  action [cos <cos>] [replace-user-priority <priority>] [discard-class <class>] [replace-dscp <dscp>]

To delete information:

no <sequence>

Input mode

```
(config-ip-qos)
```

Parameters

<sequence>

Sets the application sequence in the QoS flow list to be created or changed.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the QoS flow list.

   If conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

   Note, however, that if the maximum value for the application sequence is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{ip | <protocol> | icmp | igmp | tcp | udp }

Specifies the upper layer protocol condition for IPv4 packets.

Note that if all protocols are applicable, specify ip.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Set 0 to 255 (in decimal) or a protocol name.

   For details about the protocol names that can be specified, see "Table 28-1: Protocol names that can be specified (IPv4)".

{<source ipv4> <source ipv4 wildcard> | host <source ipv4> | any }

Specifies the source IPv4 address.

To specify all source IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <source ipv4> <source ipv4 wildcard>, host <source ipv4>, or any.

   Specify the source IPv4 address for <source ipv4>.

   For <source ipv4 wildcard>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   If host <source ipv4> is specified, the flow detection condition is an exact match of <source ipv4>.

   If any is specified, the source IPv4 address is not used as a flow detection condition.

   IPv4 address (nnn.nnn.nnn.nnn): 0.0.0.0 to 255.255.255.255

eq <source port>

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 28-3: Port names that can be specified for TCP" and "Table 28-4: Port names that can be specified for UDP (IPv4)".

If eq is specified, the flow detection condition is an exact match of <source port>.

{ <destination ipv4> <destination ipv4 wildcard> | host <destination ipv4> | any }

Specifies the destination IPv4 address.

To specify all destination IPv4 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <destination ipv4> <destination ipv4 wildcard>, host <destination ipv4>, or any. Specify the destination IPv4 address for <destination ipv4>. For <destination ipv4 wildcard>, specify a wildcard mask in IPv4 address format that specifies bits in an IPv4 address whose permitted value is arbitrary.

   If host <destination ipv4> is specified, the flow detection condition is an exact match of <destination ipv4>.

   If any is specified, the destination IPv4 address is not used as a flow detection condition.

   IPv4 address (nnn.nnn.nnn.nnn): 0.0.0.0 to 255.255.255.255

eq <destination port>

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.

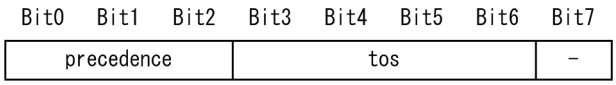
   For details about the port names that can be specified, see "Table 28-3: Port names that can be specified for TCP" and "Table 28-4: Port names that can be specified for UDP (IPv4)".

   If eq is specified, the flow detection condition is an exact match of <destination port>.

tos <tos>

Specifies 4 bits (bits 3 to 6) in the ToS field as the tos value.

The TOS value is compared with 4 bits (bits 3 to 6) in the ToS field of the sent or received packet.



1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

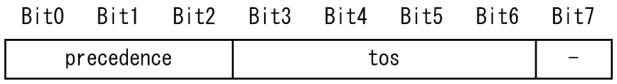
   Specify 0 to 15 (in decimal) or a tos name.

   For details about the tos names that can be specified, see "Table 28-6: tos names that can be specified".

precedence <precedence>

Specifies the precedence value, which is the first 3 bits in the ToS field.

Its value is compared with the first 3 bits in the ToS field of the sent or received packet.



1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

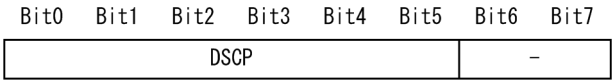
   Specify 0 to 7 (in decimal) or the precedence name.

   For details about the precedence names that can be specified, see "Table 28-7: precedence names that can be specified".

dscp <dscp>

Specifies the DSCP value, which is the first 6 bits in the ToS field.

Its value is compared with the first 6 bits in the ToS field of the received packet.



1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see "Table 28-8: 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 28-11: 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>]

This parameter is an option for using the dynamic ACL/QoS.

Specify the user class and class mask.

For <class mask>, specify the class mask that sets the bits to be compared in <class>. If <class mask> is omitted, all bits will be 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 device.

1. Default value when this parameter is omitted:

   The default CoS values are set. For details about the default Cos values, see "Configuration Guide Vol. 2, 3.5.2 CoS values and queuing priority".

2. Range of values:

   Specify 0 to 7 in decimal.

   For details about specifying Cos values, see "Configuration Guide Vol. 2, 3.5.4 Note on using priority determination".

discard-class <class>

Specifies the queuing priority.

The queuing priority of the received packet is changed to the specified <class>.

1. Default value when this parameter is omitted:

   The default queuing priority is used. For details about the default queuing priority, see "Configuration Guide Vol. 2, 3.5.2 CoS values and queuing priority".

2. Range of values:

   Specify 1 to 3 in decimal.

replace-dscp <dscp>

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the <dscp> value.

1. Default value when this parameter is omitted:

   None. (The DSCP value is not replaced.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see "Table 28-8: DSCP names that can be specified".

replace-user-priority <priority>

Specifies the value for rewriting the user priority.

Replace the user priority of the received packet with <priority>.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When 255.255.255.255 is entered for the source address wildcard mask and the destination address wildcard mask, any is displayed.
2. If nnn.nnn.nnn.nnn 0.0.0.0 is entered as the source address and the destination address, host nnn.nnn.nnn.nnn is displayed.

qos (ipv6 qos-flow-list)

Specifies flow detection conditions and action specifications in the IPv6 QoS flow list.

Syntax

To set or change information:

[<sequence>] qos {flow detection condition} [action specification]

- Flow detection conditions

  When the upper layer protocol is other than TCP, UDP, and ICMP
  {ipv6 | <protocol>} {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

  When the upper layer protocol is TCP
  tcp {<source ipv6>/<length> | host <source ipv6> | any} [eq <source port>] {<destination ipv6>/<length> | host <destination ipv6> | any} [eq <destination port>] [ack] [fin] [psh] [rst] [syn] [urg] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

  When the upper layer protocol is UDP
  udp {<source ipv6>/<length> | host <source ipv6> | any} [eq <source port>] {<destination ipv6>/<length> | host <destination ipv6> | any} [eq <destination port>] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

  When the upper layer protocol is ICMP
  icmp {<source ipv6>/<length> | host <source ipv6> | any} {<destination ipv6>/<length> | host <destination ipv6> | any} [{<icmp type> [<icmp code>] | <icmp message>}] [{traffic-class <traffic class> | dscp <dscp>}] [vlan <vlan id>] [user-priority <priority>]

- Action specification

  action [cos <cos>] [replace-user-priority <priority>] [discard-class <class>] [replace-dscp <dscp>]

To delete information:

no <sequence>

Input mode

```
(config-ipv6-qos)
```

Parameters

<sequence>

Sets the application sequence in the QoS flow list to be created or changed.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the QoS flow list.

   If conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

   Note, however, that if the maximum value for the application sequence is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{ipv6 | <protocol> | icmp | tcp | udp}

Specifies the upper layer protocol condition for IPv6 packets.

Note that if all protocols are applicable, specify ipv6.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 1 to 42, 45 to 49, 52 to 59, 61 to 255 (in decimal), or a protocol name.

   For details about the protocol names that can be specified, see "Table 28-2: Protocol names that can be specified (IPv6)".

{<source ipv6>/<length> | host <source ipv6> | any}

Specifies the source IPv6 address.

To specify all source IPv6 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <source ipv6>/<length>, host <source ipv6>, or any.

   Specify the source IPv6 address for <source ipv6>.

   For <length>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

   If host <source ipv6> is specified, the flow detection condition is an exact match of <source ipv6>.

   If any is specified, the source IPv6 address is not used as a flow detection condition.

   <source ipv6> (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):

   0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

   <length>: 0 to 128

eq <source port>

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 28-3: Port names that can be specified for TCP" and "Table 28-5: Port names that can be specified for UDP (IPv6)".

   The filter condition is an exact match of <source port>.

{<destination ipv6>/<length> | host <destination ipv6> | any}

Specifies the destination IPv6 address.

To specify all destination IPv6 addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <destination ipv6>/<length>, host <destination ipv6>, or any. Specify the destination IPv6 address for <destination ipv6>. For <length>, specify the part of the IPv6 address that is to meet the conditions by specifying the number of bits from the start of the address.

If host <destination ipv6> is specified, the flow detection condition is an exact match of <destination ipv6>.

If any is specified, the destination IPv6 address is not used as a flow detection condition.

<destination ipv6> (nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn):

0:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<length>: 0 to 128

eq <destination port>

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 28-3: Port names that can be specified for TCP" and "Table 28-5: Port names that can be specified for UDP (IPv6)".

   The filter condition is an exact match of <destination port>.

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.)

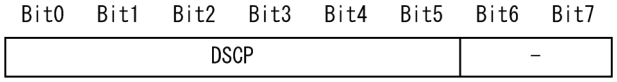
2. Range of values:

   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 28-8: 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 28-12: Message names that can be specified for ICMP (IPv6)".

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

None

vlan <vlan id>

Specifies a VLAN ID.

This parameter has an effect only when it is applied to an Ethernet interface.

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

See "Specifiable values for parameters".

user-priority <priority>

Specifies the user priority.

1. Default value when this parameter is omitted:

None. (The parameter is not set as a detection condition.)

2. Range of values:

Specify 0 to 7 in decimal.

Action parameters

action

To set or change an action parameter, you must set the action parameter keyword at the beginning of the action parameter.

1. Default value when this parameter is omitted:

None. (This action parameter keyword cannot be omitted if an action is set.)

2. Range of values:

None

cos <cos>

Specifies an index (CoS) indicating the priority on a device.

1. Default value when this parameter is omitted:

   The default CoS values are set. For details about the default Cos values, see "Configuration Guide Vol. 2, 3.5.2 CoS values and queuing priority".

2. Range of values:

   Specify 0 to 7 in decimal.

discard-class <class>

Specifies the queuing priority.

The queuing priority of the received packet is changed to the specified <class>.

1. Default value when this parameter is omitted:

   The default queuing priority is used. For details about the default queuing priority, see "Configuration Guide Vol. 2, 3.5.2 CoS values and queuing priority".

2. Range of values:

   Specify 1 to 3 in decimal.

replace-dscp <dscp>

Specifies the value for rewriting DSCP.

The DSCP field of the received packet is replaced with the <dscp> value.

1. Default value when this parameter is omitted:

   None. (The DSCP value is not replaced.)

2. Range of values:

   Specify 0 to 63 (in decimal) or the DSCP name.

   For details about the DSCP names that can be specified, see "Table 28-8: DSCP names that can be specified".

replace-user-priority <priority>

Specifies the value for rewriting the user priority.

Replace the user priority of the received packet with <priority>.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

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.

qos (mac qos-flow-list)

Specifies flow detection conditions and action specifications in the MAC QoS flow list.

Syntax

To set or change information:

[<sequence>] qos {flow detection condition} [action specification]

- Flow detection conditions

  {<source mac> <source mac mask> | host <source mac> | any}{<destination mac> <destination mac mask> | host <destination mac> | any | bpdu | cdp | lacp | lldp | oadp | pvst-plus-bpdu | slow-protocol}[<ethernet type>] [vlan <vlan id>] [user-priority <priority>] [class <class> [mask <class mask>]]

- Action specification

  action [cos <cos>] [replace-user-priority <priority>] [discard-class <class>]

To delete information:

no <sequence>

Input mode

```
(config-mac-qos)
```

Parameters

<sequence>

Specify a sequence number in the QoS flow list to be created or changed.

1. Default value when this parameter is omitted:

   10 is set as the initial value if there are no conditions in the QoS flow list.

   If conditions have been set, the initial value is the maximum value for the application sequence that has been set plus 10.

   Note, however, that if the maximum value for the application sequence is greater than 4294967284, the value cannot be omitted.

2. Range of values:

   Specify 1 to 4294967294 in decimal.

{ <source mac> <source mac mask> | host <source mac> | any }

Specifies the source MAC address. To specify all source MAC addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <source mac> <source mac mask>, host <source mac>, or any. Specify the source MAC address for <source mac>. For <source mac mask>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary. If host <source mac> is specified, the flow detection condition is an exact match of <source mac>. If any is specified, the source MAC address is not used as a flow detection condition.

   MAC address (nnnn.nnnn.nnnn): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

{<destination mac> <destination mac mask> | host <destination mac> | any | bpdu | cdp | lacp | lldp

| oadp | pvst-plus-bpdu | slow-protocol}

Specifies the destination MAC address.

To specify all destination MAC addresses, specify any.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify <destination mac> <destination mac mask>, host <destination mac>, any, bpdu, cdp, lacp, lldp, oadp, pvst-plus-bpdu, or slow-protocol.

   Specify the destination MAC address for <destination mac>. For <destination mac mask>, specify a mask in MAC address format that specifies bits in the MAC address whose permitted value is arbitrary.

   If host <destination mac> is specified, the flow detection condition is an exact match of <destination mac>.

   If any is specified, the destination MAC address is not used as a flow detection condition.

   If bpdu is specified, BPDU control packets are used as the flow detection condition.

   If cdp is specified, CDP control packets are used as the flow detection condition.

   If lacp or slow-protocol is specified, slow protocol packets are used as the flow detection condition.

   This Switch uses slow protocol packets in LACP and IEEE 802.3ah/UDLD function.

   If lldp is specified, LLDP control packets are used as the flow detection condition.

   If oadp is specified, OADP control packets are used as the flow detection condition.

   If pvst-plus-bpdu is specified, PVST+ control packets are used as the flow detection condition.

   MAC address (nnnn.nnnn.nnnn): 0000.0000.0000 to ffff.ffff.ffff (hexadecimal)

<ethernet type>

Specifies the Ethernet type value.

1. Default value when this parameter is omitted:

   None. (The parameter is not set as a detection condition.)

2. Range of values:

   Specify 0x0000 to 0xffff (hexadecimal) or the Ethernet type name. For details about the protocol names that can be specified, see "Table 28-9: 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>]

This parameter is an option for using the dynamic ACL/QoS.

Specify the user class and class mask.

For <class mask>, specify the class mask that sets the bits to be compared in <class>. If <class mask> is omitted, all bits will be 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 device.

1. Default value when this parameter is omitted:

   The default CoS values are set. For details about the default Cos values, see "Configuration Guide Vol. 2, 3.5.2 CoS values and queuing priority".

2. Range of values:

   Specify 0 to 7 in decimal.

discard-class <class>

Specifies the queuing priority.

The queuing priority of the received packet is changed to the specified <class>.

1. Default value when this parameter is omitted:

   The default queuing priority is used. For details about the default queuing priority, see "Configuration Guide Vol. 2, 3.5.2 CoS values and queuing priority".

2. Range of values:

   Specify 1 to 3 in decimal.

replace-user-priority <priority>

Specifies the value for rewriting the user priority.

Replace the user priority of the received packet with <priority>.

1. Default value when this parameter is omitted:

   None. (The user priority is not replaced.)

2. Range of values:

   Specify 0 to 7 in decimal.

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 28-10: 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.

qos-queue-group

Sets QoS queue list information for an interface (physical port).

Syntax

To set information:

qos-queue-group <qos queue list name>

To delete information:

no qos-queue-group

Input mode

```
(config-if)
```

Ethernet interface

Parameters

<qos queue list name>

Specifies the QoS queue list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string of no more than 31 alphanumeric characters with an alphabetic character for the first character.

Default behavior

PQ is set as the scheduling mode.

Impact on communication

If the scheduling mode is changed by specifying the QoS queue list name, the applicable line restarts, causing communication on the line stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the scheduling mode is changed by specifying a QoS queue list name, the new interface (a physical port) restarts. If queued packets remain in the send queue when changes are made, all packets are removed from the queue. While the packets are being removed from the queue, no new packets can be queued. You need to be careful if you logged in via a network.
2. If you did not set the scheduling mode by specifying the QoS queue list name, PQ is set as the scheduling mode.
3. If an invalid QoS queue list name is specified by using the "qos-queue-group" command, PQ is used as the scheduling mode.

qos-queue-list

Sets the scheduling mode in QoS queue list information. You can create no more than 12 lists per device.

Syntax

To set or change information:

qos-queue-list <qos queue list name> { pq | 2pq+6drr <queue1> <queue2> <queue3> <queue4> <queue5> <queue6>}

To delete information:

no qos-queue-list <qos queue list name>

Input mode

```
(config)
```

Parameters

<qos queue list name>

Specifies the QoS queue list name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a character string of no more than 31 alphanumeric characters with an alphabetic character for the first character.

{ pq | 2pq+6drr <queue1> <queue2> <queue3> <queue4> <queue5> <queue6>}

Specifies the scheduling mode.

pq

Sets priority queuing. The number of queues is fixed to 8 per 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).

2pq+6drr <queue1> <queue2> <queue3> <queue4> <queue5> <queue6>

Top-priority queues and weighted (number of packets) round robin. The number of queues is fixed to 8 per 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 byte count ratio set for <queue> for queues 6 to 1. A number from 1 to 6 suffixed to <queue> indicates the queue number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 254

Default behavior

None

Impact on communication

If the scheduling mode is changed by specifying the QoS queue list name for the "qos-queue-group" command, the applicable line restarts, causing communication on the line to stop temporarily.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the scheduling mode is changed by specifying the QoS queue list name for the "qos-queue-group" command, the new interface (physical port) restarts. If queued packets remain in the send queue when changes are made, all packets are removed from the queue. While the packets are being removed from the queue, no new packets can be queued. You need to be careful if you logged in via a network.

remark

Specifies supplementary information for a QoS flow list.

IPv4 QoS flow list, IPv6 QoS flow list, and MAC QoS flow list are available as QoS flow list. A maximum of 1024 information items can be specified for access lists and QoS flow lists per device.

Syntax

To set or change information:

remark <remark>

To delete information:

no remark

Input mode

```
(config-ip-qos)
(config-ipv6-qos)
(config-mac-qos)
```

Parameters

<remark>

Sets supplementary information about the applicable QoS flow list depending on input mode.

Only one line can be set for one QoS flow list. Entering new information overwrites the existing information.

1. Default value when this parameter is omitted:

   The initial value is null.

2. Range of values:

   Enclose a character string of no more than 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

traffic-shape rate

Sets the bandwidth by setting port bandwidth control for an interface (physical port) to limit the send bandwidth.

Syntax

To set or change information:

traffic-shape rate { <kbit/s> | <Mbit/s>M | <Gbit/s>G } [<kbyte>]

To delete information:

no traffic-shape rate

Input mode

```
(config-if)
```

Ethernet interface

Parameters

rate { <kbit/s> | <Mbit/s>M | <Gbit/s>G }

Sets port bandwidth control. Using this function limits the total-line send bandwidth to the specified bandwidth.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See the table below.

   You can specify k (default), M, or G for the unit of the value.

   Set the bandwidth so that it is equal to or smaller than the line speed.

   Table 28-14: Setting range for port bandwidth control (10/100/1000BASE-T, 1000BASE-X)

Setting unit[#1]	Setting range	Increment
Gbit/s	1 G	—
Mbit/s	1 M to 1000 M	1 Mbit/s
kbit/s	1000 to 1000000	100 kbit/s[#2]
	64 to 960	64 kbit/s[#3]

Legend: —: Not applicable

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...1000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

Table 28-15: Setting range for port bandwidth control (2.5GBASE-T)

Setting unit[#1]	Setting range	Increment
Gbit/s	1 G to 2 G	1 Gbit/s
Mbit/s	1 M to 2500 M	1 Mbit/s
kbit/s	1000 to 2500000	100 kbit/s[#2]
	64 to 960	64 kbit/s[#3]

Legend: —: Not applicable

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...1000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

Table 28-16: Setting range for port bandwidth control (10GBASE-R)

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: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...10000000).

#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

<kbyte>

Sets, in Kbytes, the burst size (tolerance to burst traffic) for port bandwidth control.

1. Default value when this parameter is omitted:

   32

2. Range of values:

   4, 8, 16, 32

Default behavior

The send bandwidth is not limited.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the set bandwidth for port bandwidth control exceeds the line speed, the port bandwidth is not controlled.
2. Depending on the chip specifications, a burst communication of about 25 milliseconds occurs when the setting value is changed.

29 Layer 2 Authentication

Configuration command and applicable Layer 2 authentication types

The following table shows the configuration command used in common for Layer 2 authentication and the applicable Layer 2 authentication types.

Table 29-1: Configuration command and applicable Layer 2 authentication types

Command name	Applicable Layer 2 authentication types		
	IEEE 802.1X	Web authentication	MAC-based authentication
authentication arp-relay	Y#	Y	Y
authentication auto-logout strayer	N	Y	Y
authentication force-authorized enable	N	Y	Y
authentication force-authorized vlan	N	Y	Y
authentication ip access-group	Y#	Y	Y
authentication logout linkdown	Y	Y	Y
authentication mac access-group	Y#	Y	Y
authentication max-user (global)	Y#	Y	Y
authentication max-user (interface)	Y#	Y	Y
authentication radius-server dead-interval	N	Y	Y

Legend:

Y: Enabled; N: Disabled

#: Can be used in the terminal authentication mode.

authentication arp-relay

Outputs ARP packets sent from unauthenticated terminals to outside the Switch.

Syntax

To set information:

authentication arp-relay

To delete information:

no authentication arp-relay

Input mode

(config-if)

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

authentication auto-logout strayer

Authentication is canceled when the Switch detects that a Web-authenticated or MAC-based authentication terminal moved to a port that is not configured for Web authentication or MAC-based authentication.

Syntax

To set information:

authentication auto-logout strayer

To delete information:

no authentication auto-logout strayer

Input mode

```
(config)
```

Parameters

None

Default behavior

Authentication is not canceled even when the Switch detects that a Web-authenticated or MAC-based authentication terminal moved to a port that is not configured for Web authentication or MAC-based authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

authentication force-authorized enable

When either of the following states exists for Web authentication and MAC-based authentication, this command forcibly changes the status of a terminal subject to authentication that requested authentication to the authenticated state:

- RADIUS authentication method is specified but there is no response from the designated RADIUS server
- Local authentication method is specified, but no authentication data exists on the device:
  - For Web authentication, this means that no users are registered in the internal Web authentication DB.
  - For MAC-based authentication, this means that no MAC addresses are registered in the internal MAC-based authentication DB.

Syntax

To set information:

authentication force-authorized enable

To delete information:

no authentication force-authorized enable

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Be especially careful when using this function, as it can pose security problems.
2. If forced authentication is performed in Web authentication dynamic VLAN mode and MAC-based authentication dynamic VLAN mode, the native VLAN of the applicable port is assigned as the post-authentication VLAN. If you want to assign a specific VLAN as the post-authentication VLAN, do so by using the "authentication force-authorized vlan" command.
3. Web authentication and MAC-based authentication separately determine whether to perform forced authentication. Therefore, forced authentication might be performed by either authentication method.

authentication force-authorized vlan

Assigns a post-authentication VLAN when forced authentication is performed on the applicable port in Web authentication dynamic VLAN mode and MAC-based authentication VLAN mode.

Syntax

To set or change information:

authentication force-authorized vlan <vlan id>

To delete information:

no authentication force-authorized vlan

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<vlan id>

Sets a MAC VLAN as the post-authentication VLAN that is assigned when forced authentication is performed.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

   Note that the default VLAN (VLAN ID = 1) cannot be specified for this command.

Default behavior

The native VLAN of the applicable port is assigned as the post-authentication VLAN.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

authentication ip access-group

For IP packets sent from an unauthenticated terminal to other terminals, only the packet types enabled by the specified IPv4 access list are forwarded to outside the Switch. Note that the Web authentication IP address is not treated as a destination IP address even when it is specified by using this command as a filtering condition.

Syntax

To set information:

authentication ip access-group {<access list number> | <access list name>}

To delete information:

no authentication ip access-group {<access list number> | <access list name>}

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{<access list number> | <access list name>}

Specifies the identifier of the IPv4 packet filter to be used to output packets to outside the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <access list number>, specify values from 100 to 199 or from 2000 to 2699 (in decimal).

   For <access list name>, specify a name that is no more than 31 characters.

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

authentication logout linkdown

When no authentication logout linkdown is set, authentication is not canceled even if the link for the port to which an authenticated terminal belongs goes down.

Syntax

To set information:

no authentication logout linkdown

To delete information:

authentication logout linkdown

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

If the link for the port to which the authenticated terminal belongs goes down, the authentication is canceled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

authentication mac access-group

For frames sent from an unauthenticated terminal to other terminals, only the frame types enabled by the specified MAC access list are forwarded to outside the Switch.

Syntax

To set information:

authentication mac access-group <access list name>

To delete information:

no authentication mac access-group <access list name>

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<access list name>

Specifies the identifier of the MAC filter to be used to output frames to outside the Switch.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify a name that is no more than 31 characters long.

   For details, see "Specifiable values for parameters".

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

authentication max-user (global)

Sets the maximum number of terminals that can be authenticated on a device for IEEE 802.1X authentication, Web authentication, and MAC-based authentication.

Syntax

To set or change information:

authentication max-user <count>

To delete information:

no authentication max-user

Input mode

```
(config)
```

Parameters

<count>

Specifies the maximum number of terminals that can be authenticated on a device for IEEE 802.1X authentication, Web authentication, and MAC-based authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1024

Default behavior

The maximum number of terminals that can be authenticated on a device is 1024.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the maximum number of terminals that can be authenticated is changed to a value smaller than the number of terminals currently authenticated, the authenticated terminals can continue communication, but no more terminals can be authenticated.
2. The maximum number of terminals that can be authenticated on a device and a port can be set at the same time.
   - If the number of authenticated terminals reaches the maximum number allowed for port-based authentication terminals, no more terminals can be authenticated on the applicable port.
   - If the number of authenticated terminals reaches the maximum number for a device, no more terminals can be authenticated on that Switch.

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)
```

Ethernet interface, port channel interface

Parameters

<count>

Specifies the maximum number of terminals that can be authenticated on the applicable port for IEEE 802.1X authentication, Web authentication, and MAC-based authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1024

Default behavior

The maximum number of authentication terminals that can be authenticated on the port is 1024.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the maximum number of terminals that can be authenticated is changed to a value smaller than the number of terminals currently authenticated, the authenticated terminals can continue communication, but no more terminals can be authenticated.
2. The maximum number of terminals that can be authenticated on a device and a port can be set at the same time.
   - If the number of authenticated terminals reaches the maximum number allowed for port-based authentication terminals, no more terminals can be authenticated on the applicable port.
   - If the number of authenticated terminals reaches the maximum number for a device, no more terminals can be authenticated on that Switch.

authentication radius-server dead-interval

Specifies how long to wait before operation is resumed on the highest-priority RADIUS server after another server was used for Web authentication and MAC-based authentication and accounting due to a communication failure with the highest-priority RADIUS server.

The highest-priority RADIUS server resumes authentication and accounting after a specified time has elapsed. That interval starts from the time that another RADIUS server starts operation.

Syntax

To set or change information:

authentication radius-server dead-interval <minutes>

To delete information:

no authentication radius-server dead-interval

Input mode

```
(config)
```

Parameters

<minutes>

Specifies, in minutes, the time that elapses before access to the highest-priority RADIUS server is made again after another RADIUS server starts operation.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1440 (minutes)

Default behavior

The highest-priority RADIUS server starts again 10 minutes after another RADIUS server starts operation.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Because Web authentication and MAC-based authentication separately access the RADIUS server to check for communication failure, either authentication method might use the highest-priority RADIUS server while the other authentication method starts using another RADIUS server.

30 IEEE 802.1X

aaa accounting dot1x default

Enables the collection of accounting information on the use of the specified authentication method. Only accounting information for IEEE 802.1X authentication is collected.

Syntax

To set information:

aaa accounting dot1x default start-stop group radius

To delete information:

no aaa accounting dot1x default

Input mode

```
(config)
```

Parameters

start-stop

If authentication is successful, the accounting start notification is sent to the accounting server. If authentication is canceled, the accounting stop notification is sent to the accounting server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

group radius

Requests accounting information for use of RADIUS server authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

aaa authentication dot1x default

Specifies IEEE 802.1X user authentication.

Syntax

To set information:

aaa authentication dot1x default group radius

To delete information:

no aaa authentication dot1x default

Input mode

```
(config)
```

Parameters

group radius

IEEE 802.1X authentication is performed by a RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If this command is not set, the RADIUS server cannot be used for IEEE 802.1X authentication.

dot1x auto-logout

The "no dot1x auto-logout" command configures the Switch to detect terminals that have been authenticated by IEEE 802.1X but have not been used for a certain period of time, and cancels authentication for these terminals.

Syntax

To set information:

no dot1x auto-logout

To delete information:

dot1x auto-logout

Input mode

```
(config)
```

Parameters

None

Default behavior

Authentication is canceled if the Switch detects that a terminal that has been authenticated by IEEE 802.1X has not been used for a certain period of time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

dot1x ignore-eapol-start

Sets the Switch not to issue EAP-Request/Identity packets in response to EAPOL-Start from a supplicant.

Syntax

To set information:

dot1x ignore-eapol-start

To delete information:

no dot1x ignore-eapol-start

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. This command can be set only on an interface for which both the "dot1x reauthentication" command and the "dot1x supplicant-detection" command (without the disable parameter) have been set.
4. This command cannot be set for an interface for which the "dot1x supplicant-detection" command with the disable parameter has been set.
5. For an interface for which this command has been set, you cannot use the "no dot1x reauthentication" command to set no re-authentication.

dot1x logging enable

Sends the IEEE 802.1X authentication action log message to the syslog server or email address (using E-Mail).

Syntax

To set information:

dot1x logging enable

To delete information:

no dot1x logging enable

Input mode

```
(config)
```

Parameters

None

Default behavior

Does not send action log messages.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To send action log messages, specify "aut" in the following command.
   - To syslog server: "logging event-kind" command
   - To an email address (using E-Mail): "logging email-event-kind" command

dot1x loglevel

Specifies the level of messages to be logged in an IEEE 802.1X action log. Use the "show dot1x logging" operation command to display the logged messages.

Syntax

To set or change information:

dot1x loglevel {error | warning | notice | info}

To delete information:

no dot1x loglevel

Input mode

```
(config)
```

Parameters

{error | warning | notice | info}

error

Only error-level log messages are logged. Only software errors are logged.

warning

Error-level and warning-level messages are logged. Detected error information, such as information about invalid frames, is logged.

notice

error-, warning-, notice-, and normal-level messages are logged. Information on whether authentication is supported, and information on server connectivity is logged.

info

error-, warning-, notice-, normal-, and info-level messages are logged. Action tracking information is also logged.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The level of messages logged in the action log is info.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.

dot1x max-req

Specifies the maximum number of EAP-Request retransmissions if the supp-timeout value is exceeded. If the number of retransmissions exceeds this value, authentication is determined to have failed.

Syntax

To set or change information:

dot1x max-req <count>

To delete information:

no dot1x max-req

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<count>

Specifies the maximum number of EAP-Request retransmissions.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The maximum number of EAP-Request retransmissions is two.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.

dot1x max-supplicant

Specifies the maximum number of terminals that can be connected to the specified interface when terminal authentication submode is set. If more terminals than this value attempt to connect, the number of terminals that can connect is restricted without attempting authentication.

Syntax

To set or change information:

dot1x max-supplicant <clients>

To delete information:

no dot1x max-supplicant

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<clients>

Specifies the maximum number of terminals that can connect to the specified interface.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 64

Default behavior

The maximum number of terminals that can be connected is 64.

Impact on communication

If the specified value is smaller than the number of terminals that are currently authenticated on the specified interface, the authentication status of all supplicants that are currently authenticated on the specified interface is canceled. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. If the specified value is smaller than the number of terminals that are currently authenticated on the specified interface, the authentication status of all supplicants that are authenticated on the specified interface is temporarily canceled.

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 multi-terminal or terminal authentication submodes are not set, single mode is used. Single mode authentication permits connection of only one terminal. When multiple terminals are connected, the status of the specified interface changes to not authenticated.

Syntax

To set information:

dot1x multiple-authentication

To delete information:

no dot1x multiple-authentication

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

The authentication submode is single mode.

Impact on communication

If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate.
4. If you set the authentication submode to multi-mode using the "dot1x multiple-hosts" command, the settings of this command are deleted.

dot1x multiple-hosts

Sets IEEE 802.1X authentication with a multi-terminal submode. Initially, only the terminal that starts authentication first is subject to authentication. After this authentication is successful, other terminals can communicate without needing to authenticate. Accordingly, multiple terminals can be connected.

If multi-terminal or terminal authentication submodes are not set, single mode is used. Single mode authentication permits connection of only one terminal. When multiple terminals are connected, the status of the specified interface changes to not authenticated.

Syntax

To set information:

dot1x multiple-hosts

To delete information:

no dot1x multiple-hosts

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

The authentication submode is single mode.

Impact on communication

If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate. Until the terminals are re-authenticated, communication is impossible.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. If the authentication submode is changed, the authentication status of the specified interface is initialized. As a result, terminals that have been authenticated need to re-authenticate.
4. If you set the authentication submode to terminal authentication mode using the "dot1x multiple-authentication" command, the settings of this command are deleted.
5. Do not set this command for a port that uses Web authentication or MAC-based authentication.

dot1x port-control

Sets the port-control status for a specified interface. Entering this command also enables the IEEE 802.1X authentication function.

Syntax

To set or change information:

dot1x port-control {auto | force-authorized | force-unauthorized}

To delete information:

no dot1x port-control

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{auto | force-authorized | force-unauthorized}

auto

IEEE 802.1X authentication is performed. The authentication result determines whether communication is enabled for terminals connected to the interface.

force-authorized

IEEE 802.1X authentication is not performed, and communication by terminals connected to the specified interface is always possible.

force-unauthorized

IEEE 802.1X authentication is not performed, and communication by terminals connected to the specified interface is never possible.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.

2. If the "dot1x multiple-hosts" or "dot1x multiple-authentication" commands have not been set, the authentication submode is single mode.
3. This command cannot be set for interfaces whose access modes or MAC VLAN modes have not been set.
4. Do not set the "dot1x port-control force-authorized" or "dot1x port-control force-unauthorized" command for an authentication port for Web authentication or MAC-based authentication.
5. If you set this command for an authentication port for Web authentication or MAC-based authentication, set the authentication submode to terminal authentication.

dot1x radius-server host

Configures the RADIUS server used for IEEE 802.1X authentication.

Syntax

To set or change information:

dot1x radius-server host {<ipv4 address> | <ipv6 address> | <host name>} [auth-port <port>] [acct-port <port>] [timeout <seconds>] [retransmit <retries>] [key <string>]

To delete information:

no dot1x radius-server host {<ipv4 address> | <ipv6 address> | <host name>}

Input mode

```
(config)
```

Parameters

{<ipv4 address> | <ipv6 address> | <host name>}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 global address of the RADIUS server in colon notation. Do not specify an IPv6 link-local address.

<host name>

Specifies the host name of the RADIUS server with 64 or fewer characters.

For details about the characters that can be specified for the host name, see "Specifiable values for parameters".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address, an IPv6 address, or a host name can be specified.

auth-port <port>

Specifies the RADIUS server port number.

1. Default value when this parameter is omitted:

   Port number 1812 is used.

2. Range of values:

   1 to 65535

acct-port <port>

Specifies the port number for RADIUS server accounting.

1. Default value when this parameter is omitted:

   Port number 1813 is used.

2. Range of values:

   1 to 65535

timeout <seconds>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   5

2. Range of values:

   1 to 30 (seconds)

retransmit <retries>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   3

2. Range of values:

   0 to 15 (times)

key <string>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   The RADIUS key set by using radius-server key is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Enclose a character string consisting of 1 to 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The RADIUS server settings registered by using the "radius-server host" command are used. If the "radius-server host" command is not registered, authentication cannot be performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is executed, the setting information of the RADIUS server referenced by IEEE 802.1X authentication has priority over the information set by using the "radius-server host" command.
2. A maximum of four RADIUS servers per device can be set by this command.
3. If multiple RADIUS servers are set by using this command, the RADIUS server listed at the top of the display resulting from this configuration command is used for the first authentication.

dot1x reauthentication

After successful IEEE 802.1X authentication, this command sets whether a supplicant is to be re-authenticated. When this command is in effect, EAP-Request/Identity packets for re-authentication are sent at the interval set by using the "dot1x timeout reauth-period" command to a supplicant as a prompt for supplicant re-authentication.

Syntax

To set information:

dot1x reauthentication

To delete information:

no dot1x reauthentication

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. For an interface for which the "dot1x ignore-eapol-start" command has been specified, you cannot use the "no dot1x reauthentication" command to set no re-authentication.

dot1x supplicant-detection

Specifies how terminal detection is performed when terminal authentication mode is specified as the authentication submode.

Syntax

To set or change information:

dot1x supplicant-detection {disable | full | shortcut | auto}

To delete information:

no dot1x supplicant-detection

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{disable | full | shortcut | auto}

Configures how terminal detection is performed when terminal authentication mode is set as the authentication submode.

disable

If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. By receiving EAPOL-Start sent by the unauthenticated terminals, the unauthenticated terminals are detected and authentication is started.

For this reason, with this parameter specified, if you use the Supplicant software that cannot send EAPOL-Start spontaneously, unauthenticated terminals cannot be detected.

full

This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the authentication sequence is not skipped.

Since authenticated terminals periodically re-authenticate, a load proportional to the number of terminals is applied. When this parameter is specified, limit the number of terminals per authentication to 20 or less to avoid the impact of load.

shortcut

This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this parameter, when authenticated terminals start re-authentication, the load is reduced by omitting the authentication sequence and immediately sending EAP-Success.

However, some Supplicant software regards sending EAP-Success immediately as an authentication failure. As a result, when this parameter is specified, communication may be interrupted immediately after authentication, communication may be interrupted several minutes to several tens of minutes after authentication, or the load may increase due to repeated re-authentication.

auto

The switch does not send an EAP-Request/Identity message to the multicast address. Instead, by receiving arbitrary frames sent by unauthenticated terminals, unauthenticated terminals are detected and authentication is started.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

shortcut is used as the behavior when a new terminal is detected.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. The "dot1x supplicant-detection" command is valid only if the "dot1x multiple-authentication" command has been set.
4. disable cannot be set for the "dot1x supplicant-detection" command on an interface for which the "dot1x ignore-eapol-start" command has been set.

dot1x system-auth-control

Enables IEEE 802.1X.

Syntax

To set information:

dot1x system-auth-control

To delete information:

no dot1x system-auth-control

Input mode

```
(config)
```

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. If the EAPOL forwarding function has been set, this command fails and IEEE 802.1X is not enabled.
3. If the "aaa authentication dot1x default group radius" command has not been set, a RADIUS server cannot be used for IEEE 802.1X authentication.

dot1x timeout keep-unauth

Specifies the period of time (in seconds) for maintaining the communication-disabled state of the interface if two or more terminals are connected to an interface on which the authentication submode is set to single mode. After the time set by using this command elapses, an authenticated terminal must be re-authenticated.

Syntax

To set or change information:

dot1x timeout keep-unauth <seconds>

To delete information:

no dot1x timeout keep-unauth

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<seconds>

Specifies the period of time (in seconds) for maintaining communication-disabled state when the authentication submode is set to single mode.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

3600 seconds is used as the period of time for maintaining the communication-disabled state.

Impact on communication

None

When the change is applied

When the communication becomes impossible.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. The value set for this command is applied only to an interface on which the authentication submode is set to single mode.

dot1x timeout quiet-period

Specifies the period of retention time (in seconds) for maintaining the unauthenticated state on the applicable interface after an IEEE 802.1X authentication failure. During this period, no EAPOL packets are sent and received EAPOL packets are ignored. Also, no authentication is performed.

Syntax

To set or change information:

dot1x timeout quiet-period <seconds>

To delete information:

no dot1x timeout quiet-period

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<seconds>

Specifies the period of retention time (in seconds) for maintaining the unauthenticated state.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

60 seconds is used as the period of retention time for maintaining the unauthenticated state.

Impact on communication

None

When the change is applied

When the Switch enters an unauthenticated state due to an authentication failure.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.

dot1x timeout reauth-period

Specifies the interval (in seconds) for re-authenticating a supplicant after a successful IEEE 802.1X authentication. EAP-Request/Identity packets for re-authentication are sent to the supplicant at the interval set by using this command as a prompt for supplicant re-authentication.

Syntax

To set or change information:

dot1x timeout reauth-period <seconds>

To delete information:

no dot1x timeout reauth-period

Input mode

(config-if)

Ethernet interface, port channel interface

Parameters

<seconds>

Specifies the interval (in seconds) for re-authenticating a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

3600 seconds is used as the interval for re-authenticating a supplicant.

Impact on communication

None

When the change is applied

- When the running timer times out (the value of the timer becomes 0.)
- When the "clear dot1x auth-state" operation command is executed to cancel authentication at the authentication level or the device level.
- When a terminal is authenticated successfully at the authentication level when there are no authenticated terminals.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. The "dot1x timeout reauth-period" command takes effect only if re-authentication has been set by using the "dot1x reauthentication" command.
4. For the parameter, set a value greater than the value set by using the "dot1x timeout tx-period" command.

dot1x timeout server-timeout

Specifies the time (in seconds) to wait for a response, including the time required for retransmitting a response to an authentication server.

Syntax

To set or change information:

dot1x timeout server-timeout <seconds>

To delete information:

no dot1x timeout server-timeout

Input mode

(config-if)

Ethernet interface, port channel interface

Parameters

<seconds>

Specifies the time (in seconds) to wait for a response.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response.

Impact on communication

None

When the change is applied

- When the running timer times out (the value of the timer becomes 0.)
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.

dot1x timeout supp-timeout

Specifies the time (in seconds) to wait for a response from a supplicant for an EAP-Request packet sent to a supplicant. If no response is received during the specified period, the EAP-Request packet is retransmitted.

Syntax

To set or change information:

dot1x timeout supp-timeout <seconds>

To delete information:

no dot1x timeout supp-timeout

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<seconds>

Specifies the time (in seconds) to wait for a response from a supplicant.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the time to wait for a response from a supplicant.

Impact on communication

None

When the change is applied

- When the running timer times out (the value of the timer becomes 0.)
- When authentication starts

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.

dot1x timeout tx-period

Specifies the interval (in seconds) for sending EAP-Request/Identity packets when IEEE 802.1X is valid.

Syntax

To set or change information:

dot1x timeout tx-period <seconds>

To delete information:

no dot1x timeout tx-period

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<seconds>

Specifies the interval (in seconds) for sending EAP-Request/Identity packets.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

30 seconds is used as the interval for sending EAP-Request/Identity packets.

Impact on communication

None

When the change is applied

- When the running timer times out (the value of the timer becomes 0.)
- When the "clear dot1x auth-state" operation command is executed to cancel authentication at the authentication level or the device level.

Notes

1. All IEEE 802.1X settings take effect when the "dot1x system-auth-control" command is set.
2. This command takes effect only if the "dot1x port-control" command has been set.
3. Specify a value smaller than the one set by using the "dot1x timeout reauth-period" command as the parameter value.

31 Web Authentication

Correspondence between configuration commands and running modes

The following table describes the Web authentication running modes in which Web authentication configuration commands can be set.

Table 31-1: Configuration commands and Web authentication running modes

Command name	Web authentication running modes	
	Fixed VLAN mode	Dynamic VLAN mode
aaa accounting web-authentication default start-stop group radius	Y	Y
aaa authentication web-authentication default group radius	Y	Y
authentication arp-relay	Y	Y
authentication auto-logout strayer	Y	Y
authentication force-authorized enable	Y	Y
authentication force-authorized vlan	—	Y
authentication ip access-group	Y	Y
authentication logout linkdown	Y	Y
authentication mac access-group	Y	Y
authentication max-user (global)	Y	Y
authentication max-user (interface)	Y	Y
authentication radius-server dead-interval	Y	Y
web-authentication auto-logout	—	Y
web-authentication connection-pool level	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	—
web-authentication logout ping ttl	Y	—
web-authentication logout polling count	Y	—
web-authentication logout polling enable	Y	—
web-authentication logout polling interval	Y	—

Command name	Web authentication running modes	
	Fixed VLAN mode	Dynamic VLAN mode
web-authentication logout polling retry-interval	Y	—
web-authentication max-timer	Y	Y
web-authentication max-user	—	Y
web-authentication port	Y	Y
web-authentication radius-server host	Y	Y
web-authentication redirect enable	Y	Y
web-authentication redirect-mode	Y	Y
web-authentication ssl connection-timeout	Y	Y
web-authentication static-vlan max-user	Y	—
web-authentication system-auth-control	Y	Y
web-authentication user replacement	Y	Y
web-authentication web-port	Y	Y

Legend:

Y: The command can be set, and the setting is applied.

—: The command can be set, but the setting is not applied.

aaa accounting web-authentication default start-stop group radius

Notifies the accounting server of the results of Web authentication.

Syntax

To set information:

aaa accounting web-authentication default start-stop group radius

To delete information:

no aaa accounting web-authentication default

Input mode

```
(config)
```

Parameters

None

Default behavior

Notification to the accounting server is only performed after this is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

aaa authentication web-authentication default group radius

Sets whether to use the RADIUS server for Web authentication function.

Syntax

To set information:

aaa authentication web-authentication default group radius

To delete information:

no aaa authentication web-authentication default

Input mode

```
(config)
```

Parameters

None

Default behavior

User authentication is performed by using the internal Web authentication DB instead of using the RADIUS server.

Impact on communication

Authentications for all users will be canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Before entering this command, set RADIUS server authentication settings.

web-authentication auto-logout

The "no web-authentication auto-logout" command configures the Switch to detect terminals that have been authenticated by Web authentication but have not been used for a certain period of time, and cancels authentication for these terminals.

Syntax

To set information:

no web-authentication auto-logout

To delete information:

web-authentication auto-logout

Input mode

```
(config)
```

Parameters

None

Default behavior

Authentication is canceled when the Switch detects that a terminal that has been authenticated by Web authentication has not been used for a certain period of time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

web-authentication connection-pool level

Sets the pool level of HTTP session connection.

Syntax

To set or change information:

web-authentication connection-pool level <level>

To delete information:

no web-authentication connection-pool level

Input mode

```
(config)
```

Parameters

<level>

Select the wait level of HTTP session connection.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 9

Default behavior

The wait level of the session connection is set to 5.

Impact on communication

None

When the change is applied

The change is applied after the "restart web-authentication web-server" operation command is used to restart the Web server.

Notes

1. The lower the value of level is set, the shorter the connection waiting time. However, as the load increases, the number of forced disconnections increases, and the Web authentication screen may not be displayed.
2. The higher the value of level is set, the fewer forced disconnections will occur. However, under heavy load, the time to wait for the Web authentication screen may increase.

web-authentication html-fileset

Set the file set name for the individual Web authentication screen 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)
```

Ethernet interface, port channel interface

Parameters

<name>

Specify the file set name registered on the Switch 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 the string with 16 or fewer characters. The characters that can be specified are alphanumeric characters (uppercase).

Default behavior

Displays the basic Web authentication screen when logging in.

Impact on communication

None

When the change is applied

The change is applied after the "restart web-authentication web-server" operation command is used to restart the Web server.

Notes

None

web-authentication ip address

Set the Web authentication IP address.

When the Web authentication IP address has been set by using this command, you can log in from an unauthenticated terminal or log out from an authenticated terminal by using the same IP address on the device.

Be sure to set this whether you are using fixed VLAN mode or dynamic VLAN mode.

This command also sets the FQDN (fully qualified domain name) corresponding to the Web authentication IP address.

Note that the IP address set by using this command is not treated as a destination IP address even when it is specified as a filtering condition by using the "authentication ip access-group" command.

Syntax

To set or change information:

web-authentication ip address <authentication address> [fqdn <fqdn>]

To delete information:

no web-authentication ip address

Input mode

```
(config)
```

Parameters

<authentication address>

Set the Web authentication IP address.

1. Default value when this parameter is omitted:
   This parameter cannot be omitted.
2. Range of values:
   Specify the IPv4 address (dot notation) for <authentication address>.
   The following values cannot be set:
   - The IP address set for the loopback interface
   - IP addresses in the subnet set for each interface

fqdn <fqdn>

Specifies the FQDN corresponding to the Web authentication IP address.

1. Default value when this parameter is omitted:
   No FQDN is set.
2. Range of values:
   Enclose a character string consisting of 1 to 255 characters in double quotation marks ("). Use only alphanumeric characters, periods (.), and hyphens (-). Note that you can use only an alphanumeric character as the first character. You do not have to enclose the character string in double quotation marks (").

Default behavior

The Web authentication IP address is not set.

Impact on communication

None

When the change is applied

The change is applied after the "restart web-authentication" operation command is used to restart the Web authentication program.

Notes

1. Because the IP address set by using this command is used exclusively for Web authentication access on a device, the IP address is not sent outside the device.
2. After this command is set or deleted, a user who is in the process of being authenticated must log in again.

web-authentication jump-url

Specifies the URL of a page to be automatically displayed after displaying the page indicating successful authentication.

Syntax

To set or change information:

web-authentication jump-url <url>

To delete information:

no web-authentication jump-url

Input mode

```
(config)
```

Parameters

<url>

Displays the page of the specified URL after the page indicating successful login is displayed.

Enter the URL starting from the first character (for example, http://.....). (See the example below.)

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string consisting of 1 to 256 characters in double quotation marks ("). Use only alphanumeric characters and special characters excluding space characters. If an input character string does not include any special characters, you do not have to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

   Examples

   (config)# web-authentication jump-url "http://www.example.com/"

Default behavior

After successful authentication, only the page indicating successful authentication is displayed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When replacing the Authentication Success page by using the "set web-authentication html-files" operation command, in the Authentication Success page file (loginOK.html), write the tag of the new URL (<!-- Redirect_URL -->) that you want the user to be redirected to after successful authentication. This causes the page specified by the URL to appear automatically after successful authentication.

web-authentication logging enable

Sends the Web authentication action log message to the syslog server or email address (using E-Mail).

Syntax

To set information:

web-authentication logging enable

To delete information:

no web-authentication logging enable

Input mode

```
(config)
```

Parameters

None

Default behavior

Does not send action log messages.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To send action log messages, specify "aut" in the following command.
   - To syslog server: "logging event-kind" command
   - To an email address (using E-Mail): "logging email-event-kind" command

web-authentication logout ping tos-windows

When Web authentication in fixed VLAN mode is used, this command sets the TOS value of special packets to cancel the authentication status of the corresponding MAC address when the special packets (ping) are received from authenticated terminals.

Syntax

To set or change information:

web-authentication logout ping tos-windows <tos>

To delete information:

no web-authentication logout ping tos-windows

Input mode

```
(config)
```

Parameters

<tos>

Sets the TOS value of special packets for Web authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 255

Default behavior

The TOS value of special packets is set to 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

web-authentication logout ping ttl

When Web authentication in fixed VLAN mode is used, this command sets the TTL value of special packets to cancel the authentication status of the corresponding MAC address when the special packets (ping) are received from authenticated terminals.

Syntax

To set or change information:

web-authentication logout ping ttl <ttl>

To delete information:

no web-authentication logout ping ttl

Input mode

```
(config)
```

Parameters

<ttl>

Sets the TTL value of special packets for Web authentication.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 255

Default behavior

The TTL value of special packets is set to 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

web-authentication logout polling count

When Web authentication in fixed VLAN mode is used, this command sets the number of times a Switch retransmits the monitoring packet that is sent periodically to check the connection status of authentication terminals when there is no response to the monitoring packet.

Syntax

To set or change information:

web-authentication logout polling count <count>

To delete information:

no web-authentication logout polling count

Input mode

```
(config)
```

Parameters

<count>

Sets the number of times a Switch retransmits a monitoring packet when there is no response to the monitoring packet.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10 (times)

Default behavior

Monitoring packets are retransmitted a maximum of three times.

Impact on communication

None

When the change is applied

The setting takes effect when the first sending interval has passed since the value was changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If link-down status for a monitored port is detected before periodic monitoring using the logout monitoring function detects no response, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time expires, the Switch stops monitoring the applicable VLAN.
4. If the number of retransmissions when a no-response state is detected is set to maximum, the number of monitoring packets increases in proportion to the number of authenticated users, and might be a heavy load on the device.

Set the polling interval by using the following formula as a guide:

Polling condition:

(1) polling interval > (2) polling retry-interval x (3) polling count

Set each value so that retransmission when a no-response state is detected does not exceed the polling interval, so that the retransmission can complete during one polling interval.

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

- To set the monitoring packet sending interval to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

web-authentication logout polling enable

Set this command to periodically check whether authenticated terminals are connected, and forcibly log out inactive or disconnected terminals when Web authentication is used in fixed VLAN mode.

Periodic monitoring is not performed if the setting of forcible logout based on periodic check is disabled by using the "no web-authentication logout polling enable" command.

Syntax

To set information:

no web-authentication logout polling enable

To delete information:

web-authentication logout polling enable

Input mode

```
(config)
```

Parameters

None

Default behavior

Authenticated terminals are monitored at the following intervals:

Polling interval

The interval set by using the "web-authentication logout polling interval" command. 300 seconds is set by default.

Retransmission interval

The interval set by using the "web-authentication logout polling retry-interval" command. One second is set by default.

Number of retransmissions

The number of retransmissions set by using the "web-authentication logout polling count" command. Three retransmissions are set by default.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If the link for the applicable port goes down, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time (set by using the "web-authentication max-timer" command) expires, the Switch stops monitoring the applicable terminal and logs it out.

4. If the sending interval time (set by using the "web-authentication logout polling interval" command) is set to the minimum value, the number of monitoring packets increases in proportion to the number of authenticated users, and might be a heavy load on the device.

   If the number of retransmissions when a no-response state is detected is set to the maximum (it is set by using the "web-authentication logout polling count" command) and the resending interval time is set to the minimum (it is set by using the "web-authentication logout polling retry-interval" command), this also might be a heavy load on the device.

   Set the polling interval by using the following formula as a guide:

   Polling condition:

   (1) polling interval > (2) polling retry-interval x (3) polling count

   Set each value so that retransmission when a no-response state is detected does not exceed the polling interval, so that the retransmission can complete during one polling interval.

   (1): web-authentication logout polling interval

   (2): web-authentication logout polling retry-interval

   (3): web-authentication logout polling count

- To set the monitoring packet sending interval to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

web-authentication logout polling interval

Sets the sending interval of monitoring packets that periodically check whether authenticated terminals are connected when Web authentication in fixed VLAN mode is used.

Syntax

To set or change information:

web-authentication logout polling interval <seconds>

To delete information:

no web-authentication logout polling interval

Input mode

```
(config)
```

Parameters

<seconds>

Sets the sending interval of monitoring packets.

The setting is configured for each device.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   60 to 86400 (seconds)

Default behavior

Monitoring packets are sent every 300 seconds to an authenticated terminal only if the logout monitoring command (the "web-authentication logout polling enable" command) has been set.

Impact on communication

None

When the change is applied

The setting takes effect when the first sending interval has passed since the value was changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If link-down status for a monitored port is detected before periodic monitoring using the logout monitoring function detects no response, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time expires, the Switch stops monitoring the applicable terminals.
4. If the sending interval is set to the minimum, the number of monitoring packets increases proportionately with the number of authenticated users, which might be a heavy load on the device.

   Set the polling interval by using the following formula as a guide:

Polling condition:

(1) polling interval > (2) polling retry-interval x (3) polling count

Set each value so that retransmission when a no-response state is detected does not exceed the polling interval, so that the retransmission can complete during one polling interval.

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

- To set the monitoring packet sending interval to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

web-authentication logout polling retry-interval

When Web authentication in fixed VLAN mode is used, this command sets the sending interval for retransmitting the monitoring packet when there is no response to a monitoring packet that periodically checks the connection status of authenticated terminals.

Syntax

To set or change information:

web-authentication logout polling retry-interval <seconds>

To delete information:

no web-authentication logout polling retry-interval

Input mode

```
(config)
```

Parameters

<seconds>

Sets the retransmission interval of monitoring packets.

The setting is configured for each device.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10 (seconds)

Default behavior

The retransmission interval of monitoring packets is one second.

Impact on communication

None

When the change is applied

The setting takes effect when the first sending interval has passed since the value was changed.

Notes

1. This command is enabled when fixed VLAN mode is set.
2. If link-down status for a monitored port is detected before periodic monitoring using the logout monitoring function detects no response, the Switch stops monitoring the terminal and logs it out due to its link-down state.
3. When the specified maximum authentication time expires, the Switch stops monitoring the applicable terminals.
4. If the retransmission interval is set to the minimum, the number of monitoring packets increases in proportion to the number of authenticated users, which might be a heavy load on the device.

   Set the polling interval by using the following formula as a guide:

Polling condition:

(1) polling interval > (2) polling retry-interval x (3) polling count

Set each value so that retransmission when a no-response state is detected does not exceed the polling interval, so that the retransmission can complete during one polling interval.

(1): web-authentication logout polling interval

(2): web-authentication logout polling retry-interval

(3): web-authentication logout polling count

- To set the monitoring packet sending interval to be shorter than 300 seconds, use the default values for the resending interval and the resending count.

web-authentication max-timer

Specifies the maximum connection time for Web-authenticated users.

Syntax

To set or change information:

web-authentication max-timer <minutes>

To delete information:

no web-authentication max-timer

Input mode

```
(config)
```

Parameters

<minutes>

Sets the maximum time (in minutes) a user is allowed for connection for authentication in the Web authentication system. After a user logs in, if the time set by using this command elapses, the authentication is automatically canceled. Cancellation of the authentication is performed within a minute after the set time elapses.

If "infinity" is specified, the maximum connection time is set to infinity, and authentication is not canceled based on the maximum connection time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 1440, or infinity

Default behavior

60 minutes is set as the maximum connection time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the value for the maximum connection time is either decreased or increased, the previous setting is applied to users that are currently authenticated, and the new configuration setting takes effect only from the next login of a new user.
2. The connection time for Web authentication is calculated using the clock in the device. Accordingly, if the date and time are changed by using the "set clock" operation command, the connection time is affected.

   Example:

   If you advance the clock by three hours, sessions will appear to have been in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, sessions will be extended by three hours.

web-authentication max-user

Sets the maximum number of users that can be authenticated in dynamic VLAN mode for Web authentication function.

Syntax

To set or change information:

web-authentication max-user <count>

To delete information:

no web-authentication max-user

Input mode

```
(config)
```

Parameters

<count>

Sets the maximum number of users that can be authenticated by Web authentication. More users than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1024

Default behavior

The maximum number of users that can be authenticated is 1024.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to users that have already been authenticated, and takes effect only from the next login.

web-authentication port

Specifies a port for which Web authentication is to be performed.

Web authentication does not work on any ports for which this command is not set.

If this command is set for an access port or a trunk port, fixed VLAN mode is set. If this command is set to a MAC VLAN, dynamic VLAN mode is set.

However, fixed VLAN mode is set for a VLAN that sends and receives tagged frames and is configured on the port on which a MAC VLAN is set.

Syntax

To set information:

web-authentication port

To delete information:

no web-authentication port

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

Web authentication is not performed for the port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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> | <host name>} [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> | <host name>}

Input mode

```
(config)
```

Parameters

{<ipv4 address> | <ipv6 address> | <host name>}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 global address of the RADIUS server in colon notation. Do not specify an IPv6 link-local address.

<host name>

Specifies the host name of the RADIUS server with 64 or fewer characters.

For details about the characters that can be specified for the host name, see "Specifiable values for parameters".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address, an IPv6 address, or a host name can be specified.

auth-port <port>

Specifies the RADIUS server port number.

1. Default value when this parameter is omitted:

   Port number 1812 is used.

2. Range of values:

   1 to 65535

acct-port <port>

Specifies the port number for RADIUS server accounting.

1. Default value when this parameter is omitted:

   Port number 1813 is used.

2. Range of values:

   1 to 65535

timeout <seconds>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   5

2. Range of values:

   1 to 30 (seconds)

retransmit <retries>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   3

2. Range of values:

   0 to 15 (times)

key <string>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   The RADIUS key set by using radius-server key is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Enclose a character string consisting of 1 to 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The RADIUS server settings registered by using the "radius-server host" command are used. If the "radius-server host" command is not registered, authentication cannot be performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is executed, the setting information of the RADIUS server referenced by Web authentication has priority over the information set by using the "radius-server host" command.
2. A maximum of four RADIUS servers per device can be set by this command.
3. If multiple RADIUS servers are set by using this command, the RADIUS server listed at the top of the display resulting from this configuration command is used for the first authentication.

web-authentication redirect enable

Sets the URL redirect function for Web authentication.

If the "no web-authentication redirect enable" command is set, URL redirection is disabled.

Syntax

To set information:

no web-authentication redirect enable

To delete information:

web-authentication redirect enable

Input mode

```
(config)
```

Parameters

None

Default behavior

If this command is omitted, the URL redirect function is enabled.

Impact on communication

None

When the change is applied

The change is applied after the "restart web-authentication web-server" operation command is used to restart the Web server.

Notes

1. This command is enabled when fixed VLAN mode or dynamic VLAN mode is set.
2. To set this command, you must also set the "web-authentication port" command.

web-authentication redirect-mode

Sets a protocol to display the Login page when the URL redirect function is enabled in Web authentication.

Syntax

To set or change information:

web-authentication redirect-mode {http | https}

To delete information:

no web-authentication redirect-mode

Input mode

```
(config)
```

Parameters

{http | https}

http

The Login page for http is displayed when the URL redirect function is enabled.

https

The Login page for https is displayed when the URL redirect function is enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The Login page for https is displayed when this command is omitted.

Impact on communication

None

When the change is applied

The change is applied after the "restart web-authentication web-server" operation command is used to restart the Web server.

Notes

1. This command is invalid if the "no web-authentication redirect enable" command is set.

web-authentication ssl connection-timeout

Sets the timeout value for SSL session establishment.

Syntax

To set or change information:

web-authentication ssl connection-timeout <seconds>

To delete information:

no web-authentication ssl connection-timeout

Input mode

```
(config)
```

Parameters

<seconds>

Sets the timeout period in seconds to wait for an SSL session to be established.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 60

Default behavior

The timeout period for SSL session establishment is 60 seconds.

Impact on communication

None

When the change is applied

The change is applied after the "restart web-authentication web-server" operation command is used to restart the Web server.

Notes

1. This configuration applies to all HTTPS requests.
2. Under heavy load, SSL connections might be disconnected frequently.
3. The actual timeout period may be longer than the value specified in this configuration.

web-authentication static-vlan max-user

Sets the maximum number of Web-authenticated users allowed in fixed VLAN mode.

Syntax

To set or change information:

web-authentication static-vlan max-user <count>

To delete information:

no web-authentication static-vlan max-user

Input mode

```
(config)
```

Parameters

<count>

Sets the maximum number of Web-authenticated users allowed in fixed VLAN mode.

More users than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1024

Default behavior

The maximum number of users that can be authenticated: 1024 users

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to users that have already been authenticated, and takes effect only from the next login.

web-authentication system-auth-control

Starts the Web authentication daemon, and enables Web authentication.

Note that if the "no web-authentication system-auth-control" command is executed, the Web authentication daemon stops.

Syntax

To set information:

web-authentication system-auth-control

To delete information:

no web-authentication system-auth-control

Input mode

```
(config)
```

Parameters

None

Default behavior

Web authentication is not performed.

Impact on communication

If the "no web-authentication system-auth-control" command is executed, authentication of the authenticated users is canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the "no web-authentication system-auth-control" command is executed, user information registered in the Web authentication DB is saved in its current state.
2. After you stop Web authentication by using the "no web-authentication system-auth-control" command, wait at least 10 seconds before using the "web-authentication system-auth-control" command to restart Web authentication.

web-authentication user replacement

Enable the user switching option.

When using one terminal with multiple user IDs, after successful authentication with the first user ID, another user ID can be used for authentication.

Syntax

To set information:

web-authentication user replacement

To delete information:

no web-authentication user replacement

Input mode

```
(config)
```

Parameters

None

Default behavior

Login with a different user name from an authenticated device is not allowed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

web-authentication web-port

Adds a TCP port number for Web authentication to any port number.

Usually, any port numbers can be added to the standard port numbers assigned for http (80) and https (443). This command can be used in either the dynamic VLAN mode or fixed VLAN mode.

Syntax

To set or change information:

web-authentication web-port {http | https} <port> [<port>]

To delete information:

no web-authentication web-port {http | https}

Input mode

```
(config)
```

Parameters

{http | https}

http

Adds a TCP port number for http.

https

Adds a TCP port number for https.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

<port>

Sets the communication port number for the http or https protocol to be added.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   832, 1024 to 65535

Default behavior

The following initial port numbers are used for communication:

- http: 80
- https: 443

Impact on communication

None

When the change is applied

The change is applied after the "restart web-authentication web-server" operation command is used to restart the Web server.

Notes

1. After this command is set or deleted, a user who is in the process of being authenticated must log in again.

32 MAC-based Authentication

Correspondence between configuration commands and running modes

The following table describes MAC-based authentication running modes in which MAC-based authentication configuration commands can be set.

Table 32-1: Configuration commands and MAC-based authentication running modes

Command name	MAC-based authentication running modes	
	Fixed VLAN mode	Dynamic VLAN mode
aaa accounting mac-authentication default start-stop group radius	Y	Y
aaa authentication mac-authentication default group radius	Y	Y
authentication arp-relay	Y	Y
authentication auto-logout strayer	Y	Y
authentication force-authorized enable	Y	Y
authentication force-authorized vlan	—	Y
authentication ip access-group	Y	Y
authentication logout linkdown	Y	Y
authentication mac access-group	Y	Y
authentication max-user (global)	Y	Y
authentication max-user (interface)	Y	Y
authentication radius-server dead-interval	Y	Y
mac-authentication auth-interval-timer	Y	Y
mac-authentication auto-logout	Y	Y
mac-authentication dot1q-vlan force-authorized	—	Y
mac-authentication dynamic-vlan max-user	—	Y
mac-authentication id-format	Y	Y
mac-authentication logging enable	Y	Y
mac-authentication login-failed-logging disable	Y	Y
mac-authentication max-timer	Y	Y
mac-authentication password	Y	Y
mac-authentication port	Y	Y
mac-authentication radius-server host	Y	Y

Command name	MAC-based authentication running modes	
	Fixed VLAN mode	Dynamic VLAN mode
mac-authentication static-vlan max-user	Y	—
mac-authentication timeout reauth-period	Y	Y
mac-authentication system-auth-control	Y	Y
mac-authentication vlan-check	Y	—

Legend:

Y: The command can be set, and the setting is applied.

—: The command can be set, but the setting is not applied.

aaa accounting mac-authentication default start-stop group radius

Notifies the accounting server of the results of MAC-based authentication.

Syntax

To set information:

aaa accounting mac-authentication default start-stop group radius

To delete information:

no aaa accounting mac-authentication default

Input mode

```
(config)
```

Parameters

None

Default behavior

Notification to the accounting server is only performed after this is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

aaa authentication mac-authentication default group radius

Sets whether to use the RADIUS server for MAC-based authentication function.

Syntax

To set information:

aaa authentication mac-authentication default group radius

To delete information:

no aaa authentication mac-authentication default

Input mode

```
(config)
```

Parameters

None

Default behavior

Authentication is performed by using the internal MAC-based authentication DB instead of using the RADIUS server.

Impact on communication

All authentications are canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Before setting this command, set RADIUS server authentication settings.

mac-authentication auth-interval-timer

Sets the time interval until the next authentication is performed for a MAC address that has failed MAC-based authentication.

Syntax

To set or change information:

mac-authentication auth-interval-timer {<minutes> | seconds <seconds>}

To delete information:

no mac-authentication auth-interval-timer

Input mode

```
(config)
```

Parameters

{<minutes> | seconds <seconds>}

Sets the time interval until the next authentication is performed after an authentication has failed once.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <minutes>, set 1 to 1440 (in minutes).

   For <seconds>, set 2 to 86400 (in seconds).

Default behavior

The time interval until the next authentication is performed is set to the default value (five minutes).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When the time is set or changed, the old setting is applied to users that have already been authenticated, and the new configuration setting takes effect only from the next authentication.
2. The connection time for MAC-based authentication is calculated using the clock in the device. Accordingly, if the date and time is changed by using the "set clock" operation command, the set time is affected.

   Example:

   If you advance the clock by three hours, sessions will appear to be in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, sessions will be extended by three hours from the set time.

mac-authentication auto-logout

The "no mac-authentication auto-logout" command configures a Switch so that the Switch detects MAC addresses that have been authenticated by MAC-based authentication but have not been used for a certain period of time, and cancels the authentication for these MAC addresses.

Alternatively, use the <delay-time> parameter to change the time from when the MAC address is no longer used until the authentication status is canceled.

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>

Specify the time period after the MAC address is no longer used until the authentication status is canceled.

1. Default value when this parameter is omitted:

   Cannot be omitted when changing information.

2. Range of values:

   60 to 86400 (seconds)

Default behavior

Authentication is canceled when the Switch detects that a MAC address that has been authenticated by MAC-based authentication has not been used for a certain period of time (3600 seconds).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

mac-authentication dot1q-vlan force-authorized

Permits terminals that send and receive tagged frames on a MAC VLAN port to communicate without being authenticated.

Syntax

To set information:

mac-authentication dot1q-vlan force-authorized

To delete information:

no mac-authentication dot1q-vlan force-authorized

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

Terminals that send and receive tagged frames on the target port are authenticated in fixed VLAN mode.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command is valid for terminals that send tagged frames destined for the VLAN ID specified with the dot1q vlan parameter of the "switchport mac" command on ports configured by the "switchport mode" command with the mac-vlan parameter.
2. Terminals permitted to communicate without authentication are treated as terminals permitted by MAC-based authentication. Therefore, consider the following:
   - Maximum number of authenticated terminals per device and per port
   - Displaying information by using an operation command

mac-authentication dynamic-vlan max-user

Sets the maximum number of MAC addresses that can be authenticated in dynamic VLAN mode of MAC-based authentication.

Syntax

To set or change information:

mac-authentication dynamic-vlan max-user <count>

To delete information:

no mac-authentication dynamic-vlan max-user

Input mode

```
(config)
```

Parameters

<count>

Sets the maximum number of MAC addresses that can be authenticated in dynamic VLAN mode of MAC-based authentication. More MAC addresses than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1024

Default behavior

The maximum number of MAC addresses that can be authenticated:

1024

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to MAC addresses that have already been authenticated, and takes effect only from the next login.

mac-authentication id-format

When using the RADIUS authentication method, set the MAC address format when requesting authentication to the RADIUS server.

The settings of this command are reflected in both the user ID and password (except when setting the "mac-authentication password" command).

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>

Set the MAC address format when requesting authentication to the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify 0 to 3. The MAC address format when specifying each value is as follows.

   0:xx-xx-xx-xx-xx-xx

   1:xxxxxxxxxxxx

   2:xxxx.xxxx.xxxx

   3:xx:xx:xx:xx:xx:xx

capitals

Specify this if the MAC address used to request authentication to the RADIUS server should be in hexadecimal uppercase format.

1. Default value when this parameter is omitted:

   It will be in hexadecimal lowercase format.

2. Range of values:

   None

Default behavior

Requests authentication to the RADIUS server with type 1 (xxxxxxxxxxxx) and in hexadecimal lowercase format.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

mac-authentication logging enable

Sends the MAC-based authentication action log message to the syslog server or email address (using E-Mail).

Syntax

To set information:

mac-authentication logging enable

To delete information:

no mac-authentication logging enable

Input mode

```
(config)
```

Parameters

None

Default behavior

Does not send action log messages.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To send action log messages, specify "aut" in the following command.
   - To syslog server: "logging event-kind" command
   - To an email address (using E-Mail): "logging email-event-kind" command

mac-authentication login-failed-logging disable

Suppresses the output of action log message when an authentication fails in MAC-based authentication.

Syntax

To set information:

mac-authentication login-failed-logging disable

To delete information:

no mac-authentication login-failed-logging disable

Input mode

```
(config)
```

Parameters

None

Default behavior

Outputs an action log message when an authentication fails in MAC-based authentication.

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 set, the output of action log messages for authentication failures will be suppressed regardless of the reason for the authentication failure in MAC-based authentication.
2. When this command is set, the output of action log message for authentication failures is suppressed even when the "mac-authentication logging enable" command is set.
3. Even if you delete this command after MAC-based authentication fails, the action log message that were suppressed will not be output.

mac-authentication max-timer

Sets the maximum connection time used for MAC-based authentication.

Syntax

To set or change information:

mac-authentication max-timer {<minutes> | infinity}

To delete information:

no mac-authentication max-timer

Input mode

```
(config)
```

Parameters

{<minutes> | infinity}

Sets the maximum connection time (in minutes) used for MAC-based authentication. After a successful authentication, if the period of time set by using this command elapses, the authentication is canceled automatically. Cancellation of the authentication is performed within a minute after the set time elapses.

If "infinity" is specified, the maximum connection time is set to infinity, and authentication is not canceled based on the maximum connection time.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 1440, or infinity

Default behavior

Authentication is not canceled based on the maximum connection time.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

If the value for the maximum connection time is either decreased or increased, the previous setting is applied to a MAC address that is currently authenticated, and the configuration setting takes effect only from the next authentication.

Notes

1. The connection time for MAC-based authentication is calculated using the clock in the device. Accordingly, if the date and time are changed by using the "set clock" operation command, the connection time is affected.

   Example:

   If you advance the clock by three hours, sessions will appear to have been in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, sessions will be extended by three hours.

mac-authentication password

Sets the password used by the terminal user when the user issues a MAC-based authentication request to the RADIUS server.

Syntax

To set or change information:

mac-authentication password <password>

To delete information:

no mac-authentication password

Input mode

```
(config)
```

Parameters

<password>

Sets the user information password for when a user issues a MAC-based authentication request to the RADIUS server.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Enclose a character string consisting of 1 to 32 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

If this command is not set, the MAC address of the terminal to be authenticated is used as the user information password.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

mac-authentication port

Specifies a port for which MAC-based authentication is to be performed.

MAC-based authentication does not work on any ports for which this command is not set.

If this command is set for an access port or a trunk port, fixed VLAN mode is set. If this command is set to a MAC VLAN, dynamic VLAN mode is set.

However, fixed VLAN mode is set for a VLAN that sends and receives tagged frames and is configured on the port on which a MAC VLAN is set.

Syntax

To set information:

mac-authentication port

To delete information:

no mac-authentication port

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

MAC-based authentication is not performed for the port.

Impact on communication

If a port subject to authentication is deleted by using this command, authentication is canceled on all applicable ports.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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> | <host name>} [auth-port <port>][acct-port <port>][timeout <seconds>][retransmit <retries>][key <string>]

To delete information:

no mac-authentication radius-server host {<ipv4 address> | <ipv6 address> | <host name>}

Input mode

```
(config)
```

Parameters

{<ipv4 address> | <ipv6 address> | <host name>}

<ipv4 address>

Specifies the IPv4 address of the RADIUS server in dot notation.

<ipv6 address>

Specifies the IPv6 global address of the RADIUS server in colon notation. Do not specify an IPv6 link-local address.

<host name>

Specifies the host name of the RADIUS server with 64 or fewer characters.

For details about the characters that can be specified for the host name, see "Specifiable values for parameters".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   An IPv4 address, an IPv6 address, or a host name can be specified.

auth-port <port>

Specifies the RADIUS server port number.

1. Default value when this parameter is omitted:

   Port number 1812 is used.

2. Range of values:

   1 to 65535

acct-port <port>

Specifies the port number for RADIUS server accounting.

1. Default value when this parameter is omitted:

   Port number 1813 is used.

2. Range of values:

   1 to 65535

timeout <seconds>

Specifies the timeout period (in seconds) for a response from the RADIUS server.

1. Default value when this parameter is omitted:

   5

2. Range of values:

   1 to 30 (seconds)

retransmit <retries>

Specifies the number of times an authentication request is resent to the RADIUS server.

1. Default value when this parameter is omitted:

   3

2. Range of values:

   0 to 15 (times)

key <string>

Specifies the RADIUS key used for encryption or for authentication of communication with the RADIUS server. The same RADIUS key must be set for the client and the RADIUS server.

1. Default value when this parameter is omitted:

   The RADIUS key set by using radius-server key is used. If no key is set, the RADIUS server is disabled.

2. Range of values:

   Enclose a character string consisting of 1 to 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

Default behavior

The RADIUS server settings registered by using the "radius-server host" command are used. If the "radius-server host" command is not registered, authentication cannot be performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is executed, the setting information of the RADIUS server referenced by MAC-based authentication has priority over the information set by using the "radius-server host" command.
2. A maximum of four RADIUS servers per device can be set by this command.
3. If multiple RADIUS servers are set by using this command, the RADIUS server listed at the top of the display resulting from this configuration command is used for the first authentication.

mac-authentication static-vlan max-user

Sets the maximum number of MAC addresses that can be authenticated in fixed VLAN mode of MAC-based authentication.

Syntax

To set or change information:

mac-authentication static-vlan max-user <count>

To delete information:

no mac-authentication static-vlan max-user

Input mode

```
(config)
```

Parameters

<count>

Sets the maximum number of MAC addresses that can be authenticated in fixed VLAN mode of MAC-based authentication. More MAC addresses than the set number cannot be authenticated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 1024

Default behavior

The maximum number of MAC addresses that can be authenticated: 1024

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command is set, the configuration setting is not applied to MAC addresses that have already been authenticated, and takes effect only from the next login.

mac-authentication system-auth-control

Starts the MAC-based authentication daemon, and enables MAC-based authentication.

Note that if the "no mac-authentication system-auth-control" command is executed, the MAC-based authentication daemon stops.

Syntax

To set information:

mac-authentication system-auth-control

To delete information:

no mac-authentication system-auth-control

Input mode

```
(config)
```

Parameters

None

Default behavior

MAC-based authentication is not performed.

Impact on communication

If the "no mac-authentication system-auth-control" command is executed, all authentications are canceled.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

mac-authentication timeout reauth-period

Specifies the interval between re-authentication attempts for authenticated terminals.

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 set to 0, the connection will continue without re-authentication.

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

The change is applied immediately after setting values are changed.

When the time is set or changed, the old setting is applied to users that have already been authenticated, and the new configuration setting takes effect only from the next authentication.

Notes

1. The connection time for MAC-based authentication is calculated using the clock in the device. Accordingly, if the date and time is changed by using the "set clock" operation command, the set time is affected.

   Example:

   If you advance the clock by three hours, sessions will appear to be in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, sessions will be extended by three hours from the set time.

mac-authentication vlan-check

When a MAC address is checked in fixed VLAN mode of MAC-based authentication, the VLAN ID is also checked.

Syntax

To set or change information:

mac-authentication vlan-check [key <string>]

To delete information:

no mac-authentication vlan-check

Input mode

```
(config)
```

Parameters

key <string>

Sets a character string to be added to the account that is used for a request to the RADIUS server in fixed VLAN mode of MAC-based authentication. For an account used by the Switch when submitting requests to the RADIUS server for MAC-based authentication function, a combination of the MAC address string, the character string set by this command, and the VLAN ID string is used.

1. Default value when this parameter is omitted:

   "%VLAN" is set.

2. Range of values:

   Enclose a character string consisting of 1 to 64 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

   Example: If "@vlan" is set, the user information (for MAC address 0012.e201.23ab, and vlan id 10) sent to the RADIUS server is 0012e20123ab@vlan10.

Default behavior

A VLAN ID is not checked for authentication.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

33 Multistep Authentication

authentication multi-step

Configure multistep authentication on the port.

Syntax

To set or change information:

authentication multi-step [{permissive | dot1x}]

To delete information:

no authentication multi-step

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{permissive | dot1x}

permissive

Both Web authentication and IEEE 802.1X are permitted for terminals for which the first step MAC-based authentication has failed.

dot1x

Allows MAC-based authentication and IEEE 802.1X as first step authentication. Web authentication is not permitted for terminals that have failed the first step MAC-based authentication or IEEE 802.1X.

1. Default value when this parameter is omitted:

   Both Web authentication and IEEE 802.1X are not permitted for terminals for which the first step MAC-based authentication has failed.

2. Range of values:

   None

Default behavior

Works as a single authentication port.

Impact on communication

Deauthenticate the terminal for the target port.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

34 DHCP snooping

ip arp inspection limit rate

Sets the maximum ARP packet reception rate (the number of ARP packets that can be received per second) per device when DHCP snooping is enabled on the Switch. ARP packets in excess of this reception rate are discarded. The actual maximum reception rate is the sum of that set by this command and that set by the "ip dhcp snooping limit rate" command. The number of packets that can be received is the total number of DHCP packets and ARP packets.

Syntax

To set or change information:

ip arp inspection limit rate <packet/s>

To delete information:

no ip arp inspection limit rate

Input mode

```
(config)
```

Parameters

<packet/s>

Sets the number of ARP packets that can be received per second.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 125 (packet/s)

Default behavior

The reception rate is not restricted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Values specified by using this command set the upper limit for the number of received packets, but do not guarantee that the Switch will work properly up to the specified number of received packets.

ip arp inspection trust

Sets the applicable interface as a trusted port where no dynamic ARP inspection is performed when DHCP snooping is enabled on a Switch.

Syntax

To set information:

ip arp inspection trust

To delete information:

no ip arp inspection trust

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

Dynamic ARP inspection is performed.

However, if the "ip dhcp snooping trust" command is set, ARP inspection is not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. On an interface on which this command is set, if the interface is accommodated in the VLAN where dynamic ARP inspection is enabled, the inspection of ARP packets is not performed.

ip arp inspection validate

Sets inspection items to be added to improve the accuracy of a dynamic ARP inspection when dynamic ARP inspections are enabled on a Switch.

Syntax

To set or change information:

ip arp inspection validate <item> [<item> [<item>]]

To delete information:

no ip arp inspection validate

Input mode

```
(config)
```

Parameters

<item> [<item> [<item>]]

Specifies an inspection item in <item>.

For <item>, select one or two of the following: src-mac, dst-mac, and ip, or set them all. You cannot set the same <item> more than once.

src-mac

When the src-mac option is specified, the Switch checks whether the source MAC address in the Layer 2 header of the received ARP packet matches the sender MAC address in the ARP header. This inspection is performed on both an ARP request and an ARP reply.

dst-mac

When the dst-mac option is specified, the Switch checks whether the destination MAC address in the Layer 2 header of the received ARP packet matches the target MAC address in the ARP header. This inspection is performed on an ARP reply.

ip

This inspection item checks if the destination IP address in the ARP header of the received ARP packet is within the following ranges:

- 1.0.0.0 to 126.255.255.255
- 128.0.0.0 to 223.255.255.255

This inspection is performed on an ARP reply only.

1. Default value when this parameter is omitted:

   At least one of them must be set. Omitted items are not inspected.

2. Range of values:

   src-mac, dst-mac, ip

Default behavior

Additional dynamic ARP inspections are not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip arp inspection vlan

Sets the VLAN used for dynamic ARP inspections when DHCP snooping is enabled on a Switch.

Syntax

To set information:

ip arp inspection vlan <vlan id list>

To change information:

ip arp inspection vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

To delete information:

no ip arp inspection vlan

Input mode

```
(config)
```

Parameters

<vlan id list>

Sets the IDs of the VLANs used for dynamic ARP inspections.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

add <vlan id list>

Adds the IDs of VLANs that will be used for dynamic ARP inspection to the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

remove <vlan id list>

Removes the IDs of the VLANs used for dynamic ARP inspections from the VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

Dynamic ARP inspections are not used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A VLAN ID for which DHCP snooping is enabled must be set for this command.

ip dhcp snooping

Enables DHCP snooping on a Switch.

Syntax

To set information:

ip dhcp snooping

To delete information:

no ip dhcp snooping

Input mode

```
(config)
```

Parameters

None

Default behavior

DHCP snooping is not used.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip dhcp snooping database url

Specifies where a binding database is to be saved.

Syntax

To set or change information:

ip dhcp snooping database url {flash | mc <file name>}

To delete information:

no ip dhcp snooping database url

Input mode

(config)

Parameters

{flash | mc <file name>}

Specifies where a binding database is to be saved.

flash

The database is saved to internal flash memory.

mc <file name>

The database is saved to a memory card.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   <file name>: A maximum of 64 characters can be set.

   Specify the name of a file on the memory card. If directories are created on a memory card by using an operation command, a maximum of 64 characters, including the directory name, can be set.

Default behavior

The binding database is not saved.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. For the save delay time set by using the "ip dhcp snooping database write-delay" command, any of the save events below causes the timer to start. When the timer expires, the binding database is saved.
   - When terminal information is dynamically registered, updated, or deleted in a binding database
   - The "ip dhcp snooping database url" command is set (this includes changes to the save destination.)
   - When the "clear ip dhcp snooping binding" operation command is executed

If the device power is turned off before the timer expires, the binding database cannot be saved.

2. If the "no ip dhcp snooping database url" command is entered after the timer set by using the "ip dhcp snooping database write-delay" command has started, the binding database is not saved.

ip dhcp snooping database write-delay

Sets the maximum save delay time to be applied when a binding database is saved.

Syntax

To set or change information:

ip dhcp snooping database write-delay <seconds>

To delete information:

no ip dhcp snooping database write-delay

Input mode

```
(config)
```

Parameters

<seconds>

Sets the maximum save delay time to be applied when a binding database is saved.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1800 to 86400 (seconds)

Default behavior

For the maximum save delay time, 6 hours (21600 seconds) is set.

Impact on communication

None

When the change is applied

The setting takes effect at the next save event after the setting value has been changed.

Notes

1. For the save delay time set by using this command, any of the save events below causes the timer to start. When the timer expires, the binding database is saved.
   - When terminal information is dynamically registered, updated, or deleted in a binding database
   - The "ip dhcp snooping database url" command is set (this includes changes to the save destination.)
   - When the "clear ip dhcp snooping binding" operation command is executed

   If the device power is turned off before the timer expires, the binding database cannot be saved.
2. If the "no ip dhcp snooping database url" command is entered after the timer set by using the "ip dhcp snooping database write-delay" command has started, the binding database is not saved.

ip dhcp snooping information option allow-untrusted

Permits untrusted ports to receive DHCP packets that have the relay agent information option (Option 82).

Syntax

To set information:

ip dhcp snooping information option allow-untrusted

To delete information:

no ip dhcp snooping information option allow-untrusted

Input mode

```
(config)
```

Parameters

None

Default behavior

DHCP packets that have the relay agent information option are discarded.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ip dhcp snooping limit rate

Sets the maximum DHCP packet reception rate (the number of DHCP packets that can be received per second) per device. DHCP packets in excess of this reception rate are discarded. The actual maximum reception rate is the sum of that set by this command and that set by the "ip arp inspection limit rate" command. The number of packets that can be received is the total number of DHCP packets and ARP packets.

Syntax

To set or change information:

ip dhcp snooping limit rate <packet/s>

To delete information:

no ip dhcp snooping limit rate

Input mode

```
(config)
```

Parameters

<packet/s>

Sets the number of DHCP packets that can be received per second.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   10 to 125 (packet/s)

Default behavior

The reception rate is not restricted.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Values specified by using this command set the upper limit for the number of received packets, but do not guarantee that the Switch will work properly up to the specified number of received packets.

ip dhcp snooping logging enable

Sends the DHCP snooping action log message to the syslog server or email address (using E-Mail).

Syntax

To set information:

ip dhcp snooping logging enable

To delete information:

no ip dhcp snooping logging enable

Input mode

```
(config)
```

Parameters

None

Default behavior

Does not send action log messages.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. To send action log messages, specify "dsn" in the following command.
   - To syslog server: "logging event-kind" command
   - To an email address (using E-Mail): "logging email-event-kind" command

ip dhcp snooping loglevel

Specifies the level of messages to be logged in a DHCP snooping action log. Use the "show ip dhcp snooping logging" operation command to display the logged messages.

Syntax

To set or change information:

ip dhcp snooping loglevel {error | warning | notice | info}

To delete information:

no ip dhcp snooping loglevel

Input mode

```
(config)
```

Parameters

{error | warning | notice | info}

error

Only error-level log messages are logged. Only software errors are logged.

warning

Error-level and warning-level log messages are logged. Detected error information, such as information of an invalid packet, is logged.

notice

Error-, warning-, and notice-level log messages are logged. Information about detected unauthorized servers is logged.

info

Error-, warning-, notice-, and info-level log messages are logged. Action tracking information is also logged.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The level of messages to be logged in an action log is notice.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Logging of messages is enabled only when the "ip dhcp snooping" command is set.

ip dhcp snooping trust

Sets whether the interface is a trusted port or an untrusted port.

Syntax

To set information:

ip dhcp snooping trust

To delete information:

no ip dhcp snooping trust

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

None

Default behavior

The applicable interface serves as an untrusted port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. On an interface on which this command is set, if the interface is accommodated in the VLAN where DHCP snooping is enabled, the inspection of DHCP packets is not performed.

ip dhcp snooping verify mac-address

Sets whether to check if the source MAC address of DHCP packets received from an untrusted port matches the client hardware addresses in the DHCP packet.

Syntax

To set information:

no ip dhcp snooping verify mac-address

To delete information:

ip dhcp snooping verify mac-address

Input mode

```
(config)
```

Parameters

None

Default behavior

The source MAC address and the client hardware address are checked to see if they match.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If this command is not set, MAC addresses are checked, so the DHCP relay agent cannot connect to an untrusted port. (This occurs because the source MAC address in the packets that passed through the DHCP relay agent has been changed.)

ip dhcp snooping vlan

Enables DHCP snooping in a VLAN. DHCP snooping is disabled if it is not set by using this command.

Syntax

To set information:

ip dhcp snooping vlan <vlan id list>

To change information:

ip dhcp snooping vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

To delete information:

no ip dhcp snooping vlan

Input mode

```
(config)
```

Parameters

<vlan id list>

Specifies the IDs of VLANs on which DHCP snooping is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

add <vlan id list>

Adds, to the VLAN list, the IDs of VLANs on which DHCP snooping is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

remove <vlan id list>

Deletes, from the VLAN list, the IDs of VLANs on which DHCP snooping is to be enabled.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to set <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

DHCP snooping is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. DHCP snooping is not valid in a VLAN in which this command has not been set.

ip source binding

Sets a static entry to the binding database.

Syntax

To set information:

ip source binding <mac address> vlan <vlan id> <ip address> interface <interface type> <interface number>

To delete information:

no ip source binding <mac address> vlan <vlan id> <ip address> interface <interface type> <interface number>

Input mode

```
(config)
```

Parameters

<mac address>

Sets the MAC address of a terminal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0000.0000.0000 to ffff.ffff.ffff

<vlan id>

Sets the ID of a VLAN to which the terminal is connected.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

<ip address>

Sets the IP address of a terminal.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1.0.0.0 to 126.255.255.255, 128.0.0.0 to 223.255.255.255

interface <interface type> <interface number>

Sets the number of the interface to which the terminal is connected.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

- Ethernet interface
- Port channel interface

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If, when entries are set, the number of binding database entries, including dynamic entries, exceeds the maximum number of entries, the entries cannot be registered in the binding database.

ip verify source

Set this command to use the terminal filter based on the DHCP snooping binding database.

The terminal filter is function used to filter the packets of unregistered source IP and MAC addresses.

Syntax

To set or change information:

ip verify source [{port-security | mac-only}]

To delete information:

no ip verify source

Input mode

(config-if)

Ethernet interface, port channel interface

Parameters

{port-security | mac-only}

Sets a terminal filter condition.

port-security

Applies the terminal filter to both the source IP and the source MAC addresses.

mac-only

Applies the terminal filter only to source MAC addresses.

1. Default value when this parameter is omitted:

   The terminal filter is applied only to source IP addresses.

2. Range of values:

   None

Default behavior

The terminal filter is not applied.

Impact on communication

If the terminal filter is applied, packets from the terminals that are not registered in the binding database are discarded regardless of the VLAN.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Terminal filters are disabled on trusted ports even when this command is set.

2. If this command is set when DHCP snooping is enabled, terminal filters are enabled even in a VLAN for which DHCP snooping is disabled.

35 Uplink Redundancy

switchport backup flush-request transmit

Enables the sending of flush control frames to upstream switches at switchover or switchback to request that the upstream switches clear their MAC address tables. This command takes effect when it is set for the primary port.

Syntax

To set or change information:

switchport backup flush-request transmit [vlan <vlan id>]

To delete information:

no switchport backup flush-request transmit

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

vlan <vlan id>

Specifies the VLAN ID of the VLAN to which flush control frames are to be sent.

1. Default value when this parameter is omitted:

   If the interface is to be set for an access port, flush control frames are sent to an access VLAN. For a trunk port, MAC VLAN port, and protocol VLAN port, flush control frames are sent to a native VLAN.

2. Range of values:

   See "Specifiable values for parameters".

Default behavior

Flush control frames are not sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set this command for the primary port. This function is not enabled when the command is set for the secondary port.
2. This function cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface for which this function is set cannot be set for a channel group. Set this function for the port channel interface to which the applicable Ethernet interface belongs.

switchport backup interface

Sets a primary port and a secondary port for uplink redundancy and the automatic switchback time.

Syntax

To set or change information:

switchport backup interface <interface type> <interface number> [preemption-delay <seconds>]

To delete information:

no switchport backup interface

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<interface type> <interface number>

Specifies a secondary port for uplink redundancy. The interface on which this command is set will be the primary port.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

   - Ethernet interface
   - Port channel interface

preemption-delay <seconds>

Sets the automatic switchback wait time. If you specify 0 seconds, a switchback is immediately performed.

1. Default value when this parameter is omitted:

   An automatic switchback is not performed.

2. Range of values:

   0 to 300 (seconds)

Default behavior

Uplink redundancy is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If this function is disabled, the ports in the standby state are also enabled for communication. This might cause loops. Shut down the primary port or the secondary port to prevent loops, and then disable this function.
2. You cannot specify an Ethernet interface that is part of a channel group as the primary port or the secondary port. Also, an Ethernet interface set as the primary port or secondary port cannot be set for a channel group. Set the primary port and secondary port for the port channel interface to which the applicable Ethernet interface belongs.

switchport backup mac-address-table update exclude-vlan

Sets the VLAN to be excluded when sending MAC address update frames.

Syntax

To set information:

switchport backup mac-address-table update exclude-vlan <vlan id list>

To change information:

switchport backup mac-address-table update exclude-vlan {<vlan id list> | add <vlan id list> | remove <vlan id list>}

To delete information:

no switchport backup mac-address-table update exclude-vlan

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<vlan id list>

Sets the VLAN to be excluded when sending MAC address update frames. If you specify multiple VLAN IDs, you can specify a range.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

add <vlan id list>

Adds a VLAN to the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

remove <vlan id list>

Removes a VLAN from the specified VLAN list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

Default behavior

MAC address update frames are sent to all VLANs included on the primary port.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, a change in the <vlan id list> value is applied the next time a switch or switchback is performed.

Notes

1. Setting the "switchport-backup mac-address-table update transmit" command enables this command.
2. Set this command for the primary port.

switchport backup mac-address-table update transmit

Enables the sending of MAC address update frames and sets the number of times the frames are sent to request that the upstream switches update their MAC address tables.

Syntax

To set or change information:

switchport backup mac-address-table update transmit [count <count>]

To delete information:

no switchport backup mac-address-table update transmit

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

count <count>

Specifies the number of times MAC address update frames are sent.

1. Default value when this parameter is omitted:

   1

2. Range of values:

   1 to 3

Default behavior

MAC address update frames are not sent.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed. However, the value set for the count parameter is applied the next time a switch or switchback is performed.

Notes

1. Set this command for the primary port.

switchport backup reset-flush-port

Specifies a port on which port resetting is performed.

Syntax

To set information:

switchport backup reset-flush-port

To delete information:

no switchport backup reset-flush-port

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Set this command for the primary port. This function is not enabled when the command is set for the secondary port.
2. This function cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface for which this function is set cannot be set for a channel group. Set this function for the port channel interface to which the applicable Ethernet interface belongs.

switchport backup reset-flush-time

Set the port-down time to be applied when port resetting is used.

Syntax

To set or change information:

switchport backup reset-flush-time <seconds>

To delete information:

no switchport backup reset-flush-time

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

<seconds>

Specifies the port-down time (in seconds) to be applied when port resetting is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10

Default behavior

The port-down time is three seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The setting of this command is enabled when the "switchport backup reset-flush-port" command has been set.

switchport-backup startup-active-port-selection

Enables the active port locking function at device startup.

Syntax

To set information:

switchport-backup startup-active-port-selection primary-only

To delete information:

no switchport-backup startup-active-port-selection

Input mode

```
(config)
```

Parameters

primary-only

Sets only the primary port as the active port at device startup.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The secondary port can also be selected as the active port at device startup.

Impact on communication

None

When the change is applied

The change is operational as soon as the setting value is changed and every time the device starts.

Notes

1. Even when this configuration has been deleted, the uplink port on which the active port locking function at device startup is running enters a state in which no active ports are set until link-up occurs on the primary port.
2. On the uplink port on which the active port locking function at device startup is running, the function to fix the active port is released if the following conditions exist:
   - Link-up occurs on the primary port.
   - An operation command is used to specify the active port as a secondary port.

36 L2 Loop Detection

loop-detection

Sets the port type for the L2 loop detection function.

Syntax

To set or change information:

loop-detection {send-inact-port | send-port | uplink-port | exception-port}

To delete information:

no loop-detection

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

{send-inact-port | send-port | uplink-port | exception-port}

send-inact-port

Sets a port as a detecting and blocking port. When an L2 loop detection frame is sent and an L2 loop detection frame sent from the local device is received, log data is output and the port is deactivated.

send-port

Sets a port as a detecting and sending port. When an L2 loop detection frame is sent and an L2 loop detection frame sent from the local device is received, log data is output.

uplink-port

Sets a port as an uplink port. No L2 loop detection frames are sent. When an L2 loop detection frame from the local device is received, log data is output to the frame source. If the port type of the frame source is a detecting and blocking port, the frame source is deactivated.

exception-port

Sets a port to be exempted from L2 loop detection. When an L2 loop detection frame is received, this will be ignored.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

The port serves as a detecting port. If an L2 loop detection frame is not sent and an L2 loop detection frame sent from the local device is detected, log data is output.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The following information is cleared when the port type is changed:
   - The number of L2 loop detection frames received until the port is deactivated
   - Time before automatic-restoration is performed
2. Even if the port type is changed, the statistics for sending and receiving L2 loop detection frames for each port are not cleared.

loop-detection auto-restore-time

Sets the time (in seconds) until a deactivated port is activated automatically.

Syntax

To set or change information:

loop-detection auto-restore-time <seconds>

To delete information:

no loop-detection auto-restore-time

Input mode

```
(config)
```

Parameters

<seconds>

Sets the time (in seconds) until a deactivated port is activated automatically.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   60 to 86400

Default behavior

A deactivated port is not reactivated automatically.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When this command has been set and the parameter is changed, if time remains until the port is activated automatically, the change becomes effective only after the remaining time has been cleared.

loop-detection enable

Enables the L2 loop detection function.

Syntax

To set information:

loop-detection enable

To delete information:

no loop-detection enable

Input mode

```
(config)
```

Parameters

None

Default behavior

The L2 loop detection function is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

loop-detection hold-time

Specifies the retention time (in seconds) that the number of received L2 loop detection frames is held before a port is changed to the inactive status. After an L2 loop detection frame is received, if the L2 loop detection retention time elapses without another L2 loop detection frame being received, the number of L2 loop detection frames received until the port is deactivated is cleared.

Syntax

To set or change information:

loop-detection hold-time <seconds>

To delete information:

no loop-detection hold-time

Input mode

```
(config)
```

Parameters

<seconds>

Specifies the retention time (in seconds) that the number of received L2 loop detection frames is held before a port is changed to the inactive status.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 86400

Default behavior

Monitors (holds) the number of L2 loop detection frames received during the hold-time interval before a port is deactivated.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The number of L2 loop detection frames received until the port is deactivated is cleared.

loop-detection interval-time

Sets the sending interval of L2 loop detection frames.

Syntax

To set or change information:

loop-detection interval-time <seconds>

To delete information:

no loop-detection interval-time

Input mode

```
(config)
```

Parameters

<seconds>

Specifies the sending interval (in seconds) of L2 loop detection frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 3600

Default behavior

The sending interval of L2 loop detection frames is 10 seconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

loop-detection threshold

Sets the number of received L2 loop detection frames before a port is deactivated.

Syntax

To set or change information:

loop-detection threshold <count>

To delete information:

no loop-detection threshold

Input mode

```
(config)
```

Parameters

<count>

Specifies the number of L2 loop detection frames that must be received before a port is deactivated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 10000

Default behavior

The number of L2 loop detection frames that must be received before a port is deactivated is 1.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the parameter is changed after this command is set, and the hold time for the number of L2 loop detection frames received has not yet expired, the hold time is reset and the new value takes effect.

37 Storm Control

storm-control

Configures the storm control function.

Syntax

To set or change information:

storm-control broadcast level pps <packet/s> [<packet/s 2>]
storm-control multicast level pps <packet/s> [<packet/s 2>]
storm-control unicast level pps <packet/s> [<packet/s 2>]
storm-control filter-broadcast <packet/s>
storm-control filter-multicast <packet/s>
storm-control filter-unicast <packet/s>
storm-control filter-recovery-time <seconds>
storm-control recovery-time <seconds>
storm-control auto-restore-time <seconds>
storm-control action { inactivate | filter }

To set information:

storm-control action trap
storm-control action log

To delete information:

no storm-control broadcast
no storm-control multicast
no storm-control unicast
no storm-control action { inactivate | 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
no storm-control recovery-time
no storm-control auto-restore-time

Input mode

```
(config-if)
```

Ethernet interface

Parameters

broadcast

Sets broadcast frames as subject to storm control.

1. Default value when this parameter is omitted:

   Broadcast frames are excluded from the storm control function.

multicast

Sets multicast frames as subject to storm control.

1. Default value when this parameter is omitted:

   Multicast frames are excluded from the storm control function.

unicast

Sets unicast frames as subject to storm control.

1. Default value when this parameter is omitted:

   Unicast frames are excluded from the storm control function.

level pps <packet/s 1> [<packet/s 2>]

<packet/s 1>

Sets the storm detection threshold (upper threshold) for the number of received frames subject to storm control. Frames that exceed the storm detection threshold are discarded. If 0 is set, all applicable frames are discarded.

<packet/s 2>

Set the value that determines when a storm has recovered after a storm has occurred (storm recovery threshold). If omitted, the storm recovery threshold works with the storm detection threshold.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See the table below.

Table 37-1: Storm detection threshold (upper threshold) and storm recovery threshold setting range and increments

Setting range (unit: packet/s)	Increments (unit: packet/s)
0 to 1500000	125#1
1500000 to 10000000	1250#2

#1

To set a value less than 1500000, specify the value in units of 125 (0, 125, 250, ..., 1499875).

#2

To set a value of 1500000 or more, specify the value in units of 1250 bit/s (1500000, 1501250, 1502500, …, 10000000).

action { inactivate | filter }

Set the behavior when a storm occurrence is detected.

inactivate

Make the target port inactive status. 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 notifications are sent.

filter

Limits the flow rate of frames received from the target port. Even if the target port belongs to a channel group, only the target port is restricted.

1. Default value when this parameter is omitted:

   If a storm is detected, only the frames exceeding the storm detection threshold are discarded. The port status does not change.

2. Range of values:

   None

action trap

Sends an SNMP notification when a storm or the end of a storm is detected.

1. Default value when this parameter is omitted:

   No SNMP notification is sent when a storm is detected.

action log

Outputs an operation message when a storm or the end of a storm is detected.

1. Default value when this parameter is omitted:

   No operation message is output when a storm is detected.

filter-broadcast <packet/s>

When restricting the flow rate of broadcast frames, set the flow rate limit value (lower threshold) for the number of broadcast frames to be relayed. Frames that exceed the flow rate limit are discarded. If 0 is set, all applicable frames are discarded.

1. Default value when this parameter is omitted:

   When flow rate is restricted, all broadcast frames are discarded.

2. Range of values:

   See the table below.

   Table 37-2: Setting range and increments of flow rate limit value (lower threshold)

Setting range (unit: packet/s)	Increments (unit: packet/s)
0 to 1500000	125
1500000 to 10000000	1250

filter-multicast <packet/s>

When restricting the flow rate of multicast frames, set the flow rate limit value (lower threshold) for the number of multicast frames to be relayed. Frames that exceed the flow rate limit are discarded. If 0 is set, all applicable frames are discarded.

1. Default value when this parameter is omitted:

   When flow rate is restricted, all multicast frames are discarded.

2. Range of values:

   See "Table 37-2: Setting range and increments of flow rate limit value (lower threshold)".

filter-unicast <packet/s>

When restricting the flow rate of unicast flooding frames, set the flow rate limit value (lower threshold) for the number of unicast flooding frames to be relayed. Frames that exceed 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 flow rate is restricted, all unicast flooding frames are discarded.

2. Range of values:

   See "Table 37-2: Setting range and increments of flow rate limit value (lower threshold)".

filter-recovery-time <seconds>

Sets the time from when a storm is detected and flow restriction starts and when the number of received frames falls below the storm recovery threshold until the flow restriction is released (flow restriction release monitoring time).

1. Default value when this parameter is omitted:

   The initial value is 1 (seconds).

2. Range of values:

   1 to 3600 (seconds)

recovery-time <seconds>

Sets the time from when a storm is detected and flow restriction starts and the number of received frames falls below the storm recovery threshold until it is determined that the storm has recovered (storm recovery monitoring time).

1. Default value when this parameter is omitted:

   The initial value is 30 (seconds).

2. Range of values:

   30 to 3600 (seconds)

auto-restore-time <seconds>

Sets the time to release inactive status on a port after a storm is detected and the port is set to the inactive status.

1. Default value when this parameter is omitted:

   After setting the port to inactive status, automatic recovery will not occur.

2. Range of values:

   30 to 86400 (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 the received frame rates exceed the set reception rate, control frames are also discarded. To prevent necessary control frames from being discarded, do not specify too small a value.
3. With action inactivate, if the port on which a storm is detected belongs to a channel group, deactivates all ports belonging to the channel group. On the other hand, even if a storm occurs on a port for which storm control is not set, storm control is not performed on any ports belonging to a channel group. Therefore, when setting storm control on a port belonging to a channel group, set storm control for all ports belonging to the channel group.
4. If the reception rate is not set for storm-control broadcast, storm-control multicast, or storm-control unicast, the action specified with storm-control action is not performed.

5. When storm-control action inactivate is set, if a storm has been detected and the port is deactivated, use the "activate" operation command to activate the port.

38 Port Mirroring

monitor session

Configures port mirroring.

Syntax

To set or change information:

monitor session <session no.> source interface <interface id list> [{rx | tx | both}] destination interface <interface type> <interface number> [encapsulation dot1q <vlan id> [ethertype <hex>]]

To change information:

monitor session <session no.> { source interface add <interface id list> | source interface remove <interface id list> }

To delete information:

no monitor session <session no.>

Input mode

```
(config)
```

Parameters

<session no.>

Specifies a port mirroring session number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 4

source interface <interface id list>

Specify a monitor port for port mirroring in list format.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

source interface add <interface id list>

Adds a monitor port for port mirroring to the list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

source interface remove <interface id list>

Deletes a monitor port for port mirroring from the list.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   See "Specifiable values for parameters".

{rx | tx | both}

Specifies the direction of the traffic subject to port mirroring.

rx

Received frames are mirrored.

tx

Sent frames are mirrored.

both

Both sent and received frames are mirrored.

1. Default value when this parameter is omitted:

   both

2. Range of values:

   None

destination interface <interface type> <interface number>

Specifies a mirror port for port mirroring. If the encapsulation dot1q parameter is not set, the port for which Layer 2 information is set cannot be specified.

<interface type> <interface number>

Specifies an interface for which a mirror port is set.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <interface type> <interface number>, you can specify the interface name and interface number corresponding to the following interface type groups. For details, see "■How to specify the interface" in "Specifiable values for parameters".

   - Ethernet interface
   - Port channel interface

encapsulation dot1q <vlan id>

Attaches a VLAN tag with the specified VLAN ID to frames to be mirrored. The VLAN ID specified by the "vlan" command and the "interface vlan" command cannot be specified.

1. Default value when this parameter is omitted:

   No VLAN tag is attached.

2. Range of values:

   2 to 4094

ethertype <hex>

Attaches a VLAN tag with the specified TPID value to frames to be mirrored.

1. Default value when this parameter is omitted:

8100

2. Range of values:

   4 digit hexadecimal number

Default behavior

None

Impact on communication

If an active line is specified as the mirror port, communication is no longer possible on the line. If a line is specified as the monitor port, communication is not affected.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. A port that has already been set as a monitor port cannot be set as a monitor port or a mirror port.
2. A port that has already been set as a mirror port cannot be set as a monitor port.
3. In a session where the encapsulation dot1q parameter is set, VLAN tags are attached to frames to be mirrored, even if a monitor port is changed or added.
4. For a port on which tag translation is set, when specifying the port as a mirror port, use the encapsulation dot1q parameter to specify a VLAN ID different from the value specified for the VLAN tag of tag translation.
5. When setting the same mirror port in multiple sessions, sessions that use the 802.1Q tagging function and sessions that do not use the 802.1Q tagging function cannot coexist.
6. The maximum number of entries separated by commas (,) in <interface id list> is 24, with or without hyphens (-).

39 sFlow Statistics

sflow destination

Specifies the IP address of the collector, which is the destination for sFlow packets.

Syntax

To set information:

sflow destination {<ip address> | <ipv6 address>} [<udp port>]

To delete information:

no sflow destination {<ip address> | <ipv6 address>} [<udp port>]

Input mode

```
(config)
```

Parameters

{<ip address> | <ipv6 address>}

Specifies the IP address of the collector, which is the destination for sFlow packets. A maximum of four sets of the IP address and UDP port can be specified.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify IP addresses in IPv4 or IPv6 format.

<udp port>

Specifies the UDP port number of the collector, which is the destination for sFlow packets.

1. Default value when this parameter is omitted:

   6343

2. Range of values:

   1 to 65535

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This parameter cannot be changed. First delete the parameter, and then add it again.
2. You can set multiple UDP port numbers for an IP address.
3. The broadcast address, multicast address cannot be set for the IPv4 and IPv6 addresses of the collector.

sflow extended-information-type

Sets whether to send flow samples in an extended data format.

Syntax

To set or change information:

sflow extended-information-type { [switch] [router] [gateway] [user] [url] | none }

To delete information:

no sflow extended-information-type

Input mode

```
(config)
```

Parameters

{ [switch] [router] [gateway] [user] [url] | none }

Sets whether to send flow samples in an extended data format.

The extended data format to be specified here is a set of network information, such as information related to switches or routers, that can be judged from packet information. For details, see "Configuration Guide Vol. 2, 19.1.3(2)(c) Extended data format".

Multiple parameters can be specified at one time. When you specify multiple parameters, separate pairs of parameters with a space character. However, note that you cannot specify any other parameters together with the none parameter.

switch

Enables the sending of switch information (such as VLAN information).

router

Enables the sending of router information (such as NextHop).

gateway

Enables the sending of gateway information (such as the AS number).

user

Enables the sending of user information (such as TACACS or RADIUS information).

url

Enables the sending of URL information.

none

No flow samples in any extended data format are to be sent to the collector.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Flow samples in any extended data format are sent to the collector.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. Any new setting of this command overwrites the old setting. If you want to change a parameter, enter all the necessary parameter values at the same time when you set this command.

sflow forward egress

Samples sent traffic on the specified port for flow samples and monitors sent and received traffic for counter samples.

Syntax

To set information:

sflow forward egress

To delete information:

no sflow forward egress

Input mode

```
(config-if)
```

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can specify either sflow forward egress or sflow forward ingress for the device. To include sent traffic in the monitoring target for flow samples, delete any sflow forward ingress commands set for other ports, and then set sflow forward egress for a port to be monitored.

sflow forward ingress

Samples received traffic on the specified port for flow samples and monitors sent and received traffic for counter samples.

Syntax

To set information:

sflow forward ingress

To delete information:

no sflow forward ingress

Input mode

```
(config-if)
```

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. You can specify either sflow forward ingress or sflow forward egress for the device. To include received traffic in the monitoring target for flow samples, delete any sflow forward egress commands set for other ports, and then set sflow forward ingress for a port to be monitored.

sflow max-header-size

Sets the maximum size from the beginning of the sample packet to be copied if the header type is used for the basic data format (see the "sflow packet-information-type" command).

Syntax

To set or change information:

sflow max-header-size <bytes>

To delete information:

no sflow max-header-size

Input mode

```
(config)
```

Parameters

<bytes>

If the header type is used for the basic data format, this parameter sets the maximum size to be copied (in bytes), starting from the beginning of the sample packet.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 256

Default behavior

A maximum of 128 bytes are copied from the beginning of the sample packet.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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

sflow packet-information-type

Sets the basic data format of the flow sample.

Syntax

To set information:

sflow packet-information-type ip

To delete information:

no sflow packet-information-type

Input mode

```
(config)
```

Parameters

ip

Sets the basic data format of the flow sample.

When ip has been specified, flow samples are sent to the collector in IPv4 format if the applicable packet is an IPv4 packet, or in IPv6 format if the applicable packet is an IPv6 packet. For details about the basic data format specified here, see "Configuration Guide Vol. 2, 19.1.3(2)(b) Basic data format".

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   None

Default behavior

Flow samples are sent to the collector in header type format.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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.

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. Recommended sampling interval values are shown in the "Sampling interval to be used as a guideline" corresponding to the total PPS in "Table 39-1: Reference sampling interval values in the operating environment". If you set a sampling interval that is significantly smaller than the recommended value, the load on the CPU might be 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: Reference sampling interval values in the operating environment

Total PPS	Sampling interval to be used as a guideline	Example configuration to be used as a guideline
Up to 25 kpps	256	
Up to 50 kpps	512	100 Mbit/s Ethernet x 1
Up to 100 kpps	1024	
Up to 200 kpps	2048	
Up to 400 kpps	4096	1 Gbit/s Ethernet x 1
Up to 800 kpps	8192	
Up to 1.6 Mpps	16384	2.5 Gbit/s Ethernet x 1

Total PPS	Sampling interval to be used as a guideline	Example configuration to be used as a guideline
Up to 3.2 Mpps	32768	
Up to 6.4 Mpps	65536	10 Gbit/s Ethernet x 1
Up to 13 Mpps	131072	
Up to 26 Mpps	262144	1 Gbit/s Ethernet x 48
Up to 52 Mpps	524288	
Up to 100 Mpps	1048576	
Up to 200 Mpps	2097152	

Table 39-2: Relationship between the entered sampling interval and the sampling interval that is actually set

Sampling interval entered in the command	Sampling interval actually set
256	256
257 to 512	512
513 to 1024	1024
1025 to 2048	2048
2049 to 4096	4096
4097 to 8192	8192
8193 to 16384	16384
16385 to 32768	32768
32769 to 65536	65536
65537 to 131072	131072
131073 to 262144	262144
262145 to 524288	524288
524289 to 1048576	1048576
1048577 to 2097152	2097152
The value must be 2097153 or greater.	2097152

Example:

If 1000 is specified for <sample count>, the value that is actually used is 1024 (= 2^10).

Default behavior

The sampling interval applied to the Switch is 2097152 (= 2^21).

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

sflow source

Specifies the IP address to be configured as the sFlow packet source (agent).

Syntax

To set or change information:

sflow source {<ip address> | <ipv6 address>}

To delete information:

no sflow source {<ip address> | <ipv6 address>}

Input mode

```
(config)
```

Parameters

{<ip address> | <ipv6 address>}

Specifies the IP address to be used as the sFlow packet source (agent). You can specify one IPv4 address or one IPv6 address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify IP addresses in IPv4 or IPv6 format.

Default behavior

If this command is not specified, the IP address is set according to the priority below. Similarly, if the specified IP address format is different from the address type specified in the "sflow destination" command, the IP address is set according to the following priority.

Priority 1

Loopback interface IP address (when using the configuration command)

Priority 2

Automatically determined from the IP addresses set for the VLAN interface of the Switch

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. The broadcast address and multicast 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 the loopback interface or VLAN interface of the Switch. If the specified IP address is not the one set for the Switch, sFlow packets cannot be sent.

sflow url-port-add

Sets the port number used for HTTP packets to a port number other than 80 when URL information is used in the extended data format.

Syntax

To set or change information:

sflow url-port-add <url port>

To delete information:

no sflow url-port-add

Input mode

```
(config)
```

Parameters

<url port>

Sets the port number used for HTTP packets to a port number other than 80 when URL information is used in the extended data format.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 65535

Default behavior

The port number used for HTTP packets is set to 80 only.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

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

40 IEEE 802.3ah/UDLD

efmoam active

Sets the port to be monitored by the IEEE 802.3ah/OAM function to active mode.

Syntax

To set or change information:

efmoam active [udld]

To delete information:

no efmoam active

Input mode

(config-if)

Ethernet interface

Parameters

udld

Specifies that the port be monitored using the IEEE 802.3ah/UDLD function and enables the unidirectional link failure detection function.

1. Default value when this parameter is omitted:

   The unidirectional link failure detection function is not executed on the applicable port.

2. Range of values:

   None

Default behavior

The applicable port works in passive mode and does not detect a unidirectional link failure.

Impact on communication

If this function is enabled and a line failure is detected, the applicable port is deactivated.

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the udld parameter is not set on both connected ports, link failures cannot be detected by using this function.

efmoam disable

Enables or disables the IEEE 802.3ah/OAM function on a device.

To disable the IEEE 802.3ah/OAM function, set the "efmoam disable" command.

To enable the IEEE 802.3ah/OAM function again, set the "no efmoam disable" command.

In passive mode, the send process starts when an OAMPDU from the active mode is received.

Syntax

To set information:

efmoam disable

To delete information:

no efmoam disable

Input mode

```
(config)
```

Parameters

None

Default behavior

The IEEE 802.3ah/OAM function is enabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

efmoam udld-detection-count

Sets the number of OAMPDU response timeouts that must occur to recognize a failure. (The OAMPDU is a monitoring packet of the IEEE 802.3ah/UDLD function.)

Syntax

To set or change information:

efmoam udld-detection-count <count>

To delete information:

no efmoam udld-detection-count

Input mode

```
(config)
```

Parameters

<count>

Specifies the number of OAMPDU response timeouts that must occur to determine that a line failure has occurred when timeouts occur repeatedly. When the occurrence reaches the specified number of times, the applicable port is deactivated.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   3 to 300

Default behavior

30 is used as the number of times for determining a line failure.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If a value smaller than the initial value is set, a unidirectional link failure might be falsely detected.

41 CFM

domain name

Sets the name used for a domain.

Syntax

To set or change information:

domain name {no-present | str <strings> | dns <name> | mac <mac> <id>}

To delete information:

no domain name

Input mode

```
(config-ether-cfm)
```

Parameters

{no-present | str <strings> | dns <name> | mac <mac> <id>}

Sets the parameter to be used as the domain name.

no-present

If this parameter is set, the Maintenance Domain Name field in CCM is not used.

str <strings>

Uses a character string of no more than 43 characters to specify a domain name.

dns <name>

Uses the domain name server name as the domain name.

mac <mac> <id>

Uses the MAC address and a 2-byte ID as a domain name.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <strings>, enclose a character string consisting of no more than 43 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

   For <name>, specify a host name with no more than 63 characters. For details about the characters that can be specified, see "Specifiable values for parameters".

   For <mac>, specify a value from 0000.0000.0000 to feff.ffff.ffff. Note, however, that a multicast MAC address (address whose first-byte lowest bit is set to 1) cannot be set.

   For <id>, specify a value from 0 to 65535.

Default behavior

no-present is set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. When a parameter other than no-present has been specified, if a character string with more than 43 characters is specified for the str <strings> parameter in the "ma name" command, the first character of the specified parameter is added to CCM.

ethernet cfm cc alarm-priority

Sets the failure level detected by the CC function. A failure that exceeds the set failure level is to be detected.

Syntax

To set or change information:

ethernet cfm cc level <level> ma <no.> alarm-priority <priority>

To delete information:

no ethernet cfm cc level <level> ma <no.> alarm-priority

Input mode

```
(config)
```

Parameters

level <level>

Specifies the domain level that has been set by using the "ethernet cfm domain" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <no.>

Specifies an MA ID number that has been set by using the "ma name" command or the "ma vlan-group" command. Even if the "ma name" command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<priority>

Sets the lowest failure level that will be detected by CC.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 5

   The following table describes the failure descriptions corresponding to the setting values.

   Table 41-1: Failure descriptions corresponding to the setting values

Setting value	Failure type	Display in a command	Failure description
0	none	—	No failure was detected.
1	DefRDICCM	RDI	A CCM with the failure flag on was received.

Setting value	Failure type	Display in a command	Failure description
2	DefMACstatus	PortState	A received CCM has information about whether a port or interface is in the down status.
3	DefRemoteCCM	Timeout	A CCM from a remote MEP has timed out.
4	DefErrorCCM	ErrorCCM	A MEP configuration error has occurred, or a CCM with an abnormal sending interval was received.
5	DefXconCCM	OtherCCM	A CCM with a different MA was received.

Default behavior

Level 2 or higher failures are detected.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ethernet cfm cc alarm-reset-time

If CC detects repeated failures, this sets the time interval within which the CC function recognizes that this is a redetected failure. After detecting a failure, if another failure is detected within the time interval set by using this command, the failure is treated as a redetected failure and no SNMP notification is sent.

However, if the level of the redetected failure is higher than that of the previously-detected failure, an SNMP notification is sent.

Syntax

To set or change information:

ethernet cfm cc level <level> ma <no.> alarm-reset-time <time>

To delete information:

no ethernet cfm cc level <level> ma <no.> alarm-reset-time

Input mode

```
(config)
```

Parameters

level <level>

Specifies the domain level that has been set by using the "ethernet cfm domain" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <no.>

Specifies an MA ID number that has been set by using the "ma name" command or the "ma vlan-group" command. Even if the "ma name" command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<time>

Sets the period of time until the CC function recognizes that the failure is a redetected failure. The actual value used is set in 500 millisecond increments (a value less than 500 milliseconds is rounded up to 500 milliseconds).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2500 to 10000 (milliseconds)

Default behavior

The period of time until the CC function recognizes that the failure is a redetected failure is set to 10000 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ethernet cfm cc alarm-start-time

Sets the time from the point at which CC detects a failure until it sends an SNMP notification.

Syntax

To set or change information:

ethernet cfm cc level <level> ma <no.> alarm-start-time <time>

To delete information:

no ethernet cfm cc level <level> ma <no.> alarm-start-time

Input mode

```
(config)
```

Parameters

level <level>

Specifies the domain level that has been set by using the "ethernet cfm domain" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <no.>

Specifies an MA ID number that has been set by using the "ma name" command or the "ma vlan-group" command. Even if the "ma name" command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<time>

Sets the time from the point at which CC detects a failure until it sends an SNMP notification. The actual value used is set in 500 millisecond increments (a value less than 500 milliseconds is rounded up to 500 milliseconds).

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2500 to 10000 (milliseconds)

Default behavior

The time from the point at which CC detects a failure until it sends an SNMP notification is 2500 milliseconds.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ethernet cfm cc enable

Sets in a domain an MA in which the CC function is used.

If the "ethernet cfm mep" command has already been set, sending from the applicable port to CCM starts.

Syntax

To set information:

ethernet cfm cc level <level> ma <no.> enable

To delete information:

no ethernet cfm cc level <level> ma <no.> enable

Input mode

```
(config)
```

Parameters

level <level>

Specifies the domain level that has been set by using the "ethernet cfm domain" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <no.>

Specifies an MA ID number that has been set by using the "ma name" command or the "ma vlan-group" command. Even if the "ma name" command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

Default behavior

Monitoring by CC is not performed.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ethernet cfm cc interval

Sets the CCM sending interval for a target MA.

Syntax

To set or change information:

ethernet cfm cc level <level> ma <no.> interval {1s | 10s | 1min | 10min}

To delete information:

no ethernet cfm cc level <level> ma <no.> interval

Input mode

```
(config)
```

Parameters

level <level>

Specifies the domain level that has been set by using the "ethernet cfm domain" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <no.>

Specifies an MA ID number that has been set by using the "ma name" command or the "ma vlan-group" command. Even if the "ma name" command is used to specify the MA name, using a character string, or a VLAN ID, this parameter specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

{1s | 10s | 1min | 10min}

Sets the CCM sending interval.

1s

Sets the CCM sending interval to 1 seconds.

10s

Sets the CCM sending interval to 10 seconds.

1min

Sets the CCM sending interval to 1 minutes.

10min

Sets the CCM sending interval to 10 minutes.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

None

Default behavior

1min is used as the CCM sending interval.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the CCM sending interval is set to a shorter value than the initial value, the CPU usage of the device becomes higher, which might affect communication.

ethernet cfm domain

Sets a domain. Executing this command switches to config-ether-cfm mode in which the domain name and MA can be set.

Syntax

To set information:

ethernet cfm domain level <level> [direction-up]

To delete information:

no ethernet cfm domain level <level>

Input mode

```
(config)
```

Parameters

level <level>

Specifies the domain level.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

direction-up

When up/down is not explicitly set by using the "ethernet cfm mep" command, you can set this parameter to have the Switch work in Up MEP mode.

1. Default value when this parameter is omitted:

   The Switch works in Down MEP mode.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If any of the following commands references a domain set by using this command, this command cannot be deleted:
   - ethernet cfm cc enable

- ethernet cfm mep
- ethernet cfm mip

ethernet cfm enable (global)

Starts CFM.

Syntax

To set information:

ethernet cfm enable

To delete information:

no ethernet cfm enable

Input mode

```
(config)
```

Parameters

None

Default behavior

CFM does not work even if another CFM command has been set.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ethernet cfm enable (interface)

When no ethernet cfm enable is set, CFM PDU transmission processing on the applicable port or the applicable port channel stops.

Syntax

To set information:

no ethernet cfm enable

To delete information:

ethernet cfm enable

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

None

Default behavior

CFM PDUs can be received.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

ethernet cfm mep

Sets a MEP used by the CFM function.

Syntax

To set information:

ethernet cfm mep level <level> ma <no.> mep-id <mepid> [{down | up}]

To delete information:

no ethernet cfm mep level <level> ma <no.> mep-id <mepid>

Input mode

`(config-if)`

Ethernet interface, port channel interface

Parameters

level <level>

Specifies the domain level that has been set by using the "ethernet cfm domain" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

ma <no.>

Specifies an MA ID number that has been set by using the "ma name" command or the "ma vlan-group" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

mep-id <mepid>

Sets the MEP ID.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   1 to 8191

3. Note on using this parameter:

   Set a value unique within the MA.

{down | up}

Specifies the direction of a domain.

down

Sets the MEP as Down MEP so that the line side will be maintained.

up

Sets the MEP as Up MEP so that the relay side (toward the device) will be maintained.

1. Default value when this parameter is omitted:

   When direction-up has been set by using the "ethernet cfm domain" command, Up MEP is used. If it has not been set, Down MEP is used.

2. Range of values:

   None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the "ethernet cfm mip" command is set on the same interface, a domain level equal to or higher than the "ethernet cfm mip" command cannot be specified.
2. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

ethernet cfm mip

Sets a MIP used by the CFM function.

Syntax

To set information:

ethernet cfm mip level <level>

To delete information:

no ethernet cfm mip level <level>

Input mode

```
(config-if)
```

Ethernet interface, port channel interface

Parameters

level <level>

Specifies the domain level that has been set by using the "ethernet cfm domain" command.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 7

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

1. If the "ethernet cfm mep" command is set on the same interface, a domain level equal to or lower than the "ethernet cfm mep" command cannot be specified.
2. This command cannot be set for an Ethernet interface that is set for a channel group. Also, an Ethernet interface set by using this command cannot be set for a channel group. Set this command for the port channel interface to which the applicable Ethernet interface belongs.

ma name

Sets the name of an MA to be used in the applicable domain.

Syntax

To set or change information:

ma <no.> name {str <strings> | vlan <vlan id>}

To delete information:

no ma <no.> name

Input mode

```
(config-ether-cfm)
```

Parameters

<no.>

Specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

{str <strings> | vlan <vlan id>}

Specifies the name of an MA by using a character string or a VLAN ID.

str <strings>

A character string specified for <strings> is used for the name of an MA.

vlan <vlan id>

The VLAN ID specified for <vlan id> is used as the name of the MA.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For <strings>, enclose a character string consisting of no more than 45 characters in double quotation marks ("). Specifiable characters are alphanumeric characters and special characters. To enter a character string that does not include any special characters such as a space, you do not need to enclose the character string in double quotation marks ("). For details, see "■Arbitrary character string" in "Specifiable values for parameters".

   Specify a value from 1 to 4095 for <vlan id>.

3. Note on using this parameter:

   • If a parameter other than no-present has been set by using the "domain name" command and you specify a character string of 44 characters or more for <strings>, the 44th and subsequent characters are not used in the Short MA Name field in the CCM.

   • <strings> or <vlan id> that has already been set in the same domain cannot be specified.

Default behavior

<no.> of the "ma vlan-group" command is used for a name of an MA.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

ma vlan-group

Sets the VLAN belonging to the MA used in a domain.

Syntax

To set or change information:

ma <no.> vlan-group <vlan id list> [primary-vlan <vlan id>]

To delete information:

no ma <no.> vlan-group

Input mode

```
(config-ether-cfm)
```

Parameters

<no.>

Specifies the MA ID number.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   0 to 65535

<vlan id list>

Specifies the VLANs to be used in the applicable MA.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   For details about how to specify <vlan id list> and the specifiable range of values, see "Specifiable values for parameters".

primary-vlan <vlan id>

Specifies the primary VLAN to be used when CFM PDUs are sent in the applicable MA.

1. Default value when this parameter is omitted:

   From the VLAN list specified by using vlan-group <vlan id list>, a lower-numbered VLAN is used as the primary VLAN.

2. Range of values:

   1 to 4094

3. Note on using this parameter:

   Specify the VLAN IDs specified by using vlan-group <vlan id list>.

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

42 LLDP

lldp enable

Enables operation of LLDP for a port.

Syntax

To set information:

lldp enable

To delete information:

no lldp enable

Input mode

`(config-if)`

Ethernet interface

Parameters

None

Default behavior

None

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

lldp hold-count

Specifies how long the LLDP frames sent from the Switch to neighboring devices will be retained on the neighboring devices.

Syntax

To set or change information:

lldp hold-count <count>

To delete information:

no lldp hold-count

Input mode

```
(config)
```

Parameters

<count>

Specifies the scaling for the value specified by the "lldp interval-time" command as the time that a neighboring device retains the LLDP frame sent from the Switch. If the time exceeds 65535, which is the maximum value, 65535 is used.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   2 to 10

Default behavior

4 is set as the time that a neighboring device retains LLDP frames sent from the Switch.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

lldp interval-time

Specifies the sending interval at which the Switch sends LLDP frames.

Syntax

To set or change information:

lldp interval-time <seconds>

To delete information:

no lldp interval-time

Input mode

```
(config)
```

Parameters

<seconds>

Specifies the sending interval (in seconds) at which the Switch sends LLDP frames.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   5 to 32768

Default behavior

30 seconds is used as the sending interval at which the Switch sends LLDP frames.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

lldp management-address

Sets the LLDP management address.

Syntax

To set or change information:

lldp management-address {ip <ip address> | ipv6 <ipv6 address>}

To delete information:

no lldp management-address

Input mode

```
(config)
```

Parameters

{ip <ip address> | ipv6 <ipv6 address>}

Specify the management address.

1. Default value when this parameter is omitted:

   This parameter cannot be omitted.

2. Range of values:

   Specify an IPv4 or IPv6 address.

Default behavior

Neighboring devices are not notified of the management address.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

lldp run

Enables the LLDP function.

Syntax

To set information:

lldp run

To delete information:

no lldp run

Input mode

(config)

Parameters

None

Default behavior

The LLDP function is disabled.

Impact on communication

None

When the change is applied

The change is applied immediately after setting values are changed.

Notes

None

43 Error Messages Displayed When Editing the Configuration

43.1 Error messages displayed when editing the configuration

43.1.1 Common

Table 43-1: Common error messages

Message	Description
<value1> has already been set -- <value2>.	<value1> information has already been set. <value2> could not be set. Delete <value1> information or check if information you expected is set.
<value1> has already been set.	<value1> information has already been set. Delete <value1> information or check if information you expected is set.
Can not change it because data is not corresponding.	Cannot be changed because there is no matching data. Check if information to be changed exists.
Can not delete it because data is not corresponding.	Data cannot be deleted because there is no matching data or duplicated data is specified. Check if there is data to be deleted or duplicated data is specified.
Can't delete this configuration referred by other configuration.	This configuration cannot be changed because it is specified by another configuration. Delete the configuration that refers to this configuration, and then retry the deletion.
Interface not found.	The specified interface cannot be found. Check the interface setting.
Invalid IPv4 address. -- <value1>	<value1> is outside the valid IPv4 address range. Set a value within the range.
	<value1>: Invalid value
Invalid line type.	The line type is invalid.
Invalid port number. -- <value1>	<value1> is outside the valid port number range. Set a value within the range.
	<value1>: Invalid value
Invalid Mask. -- <value1>	<value1> is outside the valid subnet mask range. Set a value within the range.
	<value1>: Invalid value
Maximum number of entries are already defined (config memory shortage). <value1>	Shared memory for the configuration is full. Delete entries that are no longer needed, execute the "save" command, and then add an entry.
	<value1>: Entry name

Message	Description
Maximum number of entries are already defined. <value1>	An attempt is being made to set a configuration that is larger than the capacity limit or to change a configuration in an environment already at the maximum capacity limit. Delete configurations that are no longer used, and then set the configuration again.
	<value1>: Entry name for the maximum capacity limit
Not found <value1>.	The specified <value1> information could not be found. Check if the <vlaue1> information has been set.
Syntax error -- <value1>.	The configuration syntax or the value is invalid. Set the configuration again with the correct syntax or value.
	<value1>: Invalid value
The different name is already defined.	A different name is already set.
The sequence number exceeded the maximum value. Try "resequence" Command.	The sequence number exceeds the maximum value. To specify an entry, execute the "resequence" command, and then specify this entry again.
This configuration has already been set.	This configuration has already been set.
Too long value or illegal format (max <value1> characters).	The number of characters exceeds the maximum value (<value1>), or an invalid character is contained. Use the determined format.
	<value1>: Number of characters that can be entered
Too long value or illegal format (max <value1> digit number).	The number of characters you entered exceeds the maximum number of digits (<value1>), or an invalid character exists. Use the determined format.
	<value1>: Number of digits that can be entered

43.1.2 Configuration editing and operation information

Table 43-2: Error messages displayed while editing and operating configurations

Message	Description
<process> is starting. Please try again.	A program is being started. Wait a while, and then re-execute the command.
	<process>: Program name
A specified number of interfaces exceeds the limitation.	The interface cannot be set because the number of interfaces exceeds the maximum value.
Can't execute config command, please try again.	A communication error occurred between processes. Wait a while, and then re-execute the command.
Configuration command syntax error.line <line number> : "<error syntax>"	A configuration command of the source file has a syntax error.
	<line number>: Number of lines in a copy file <error syntax>: Error syntax

Message	Description
Configuration data cannot temporarily delete. Please try again.	Deletion is not permitted temporarily because the configuration you entered is not completed. Wait a while, and then re-execute the command.
Configuration file is empty.	There are no contents in the configuration.
Data transfer failed. (<reason>)	Transferring the configuration file to the remote server failed. Re-execute the command with the debug parameter specified for checking.
	<reason>: Additional information
File format error.	The file format is invalid. Make sure the name of the specified file is correct.
File name is a directory.	A directory name cannot be specified. Specify a file name.
File name too long.	The specified file name is too long. Shorten the file name.
Filename or directory path is too long.	The path to the target is too long. Shorten the path length.
Logical inconsistency occurred.	A conflict occurred in the configuration. Take the following actions. If the following cases do not apply, wait a while, and then re-execute the command. • If you are editing data in a level-2 or level-3 configuration command mode, use the "show running-config" operation command to check whether the command that switched to the target command mode was deleted. • If you interrupted the "end" or "quit (exit)" command by pressing Ctrl + C, and then executed the configuration command, use the "end" command to exit the configuration command mode. • If you execute a configuration command while the device is restarting, re-execute the command after the device is restarted.
No enough parameters.	No parameters are specified. Specify the necessary parameters.
No such file or directory.	The specified file or directory is not found. Specify the correct file name or directory name.
Not enough memory, configuration file is too big.	There is not enough memory to save the configuration because it is too large.
Not enough space on device.	Capacity at the write destination is insufficient. Delete files that are no longer needed.
Now configuration data is changing. Please try again.	The configuration you entered cannot be edited because it is not completed. Wait a while, and then re-execute the command.
Permission denied.	You do not have write permission for the target.
Resource temporarily unavailable.	Resource is temporarily insufficient. Wait a while, and then re-execute the command.

Message	Description
The command execution failed, because another command executing.	The command cannot be executed because it conflicts with a command which is being executed.
The command execution failed, because configuration file is editing.	This command cannot be executed because another user is editing the configuration.
The command execution failed, because configuration file is saving.	No edit command can be executed while saving the configuration.
The command execution failed, because multiple commands can not execute simultaneously.	Multiple commands cannot be executed concurrently.
The saving command is being executed, please try again.	The operation is not permitted because the "save" command is being executed. Wait a while, and then re-execute the command.
This configuration is active.	This configuration matches the implementation and cannot be changed.

43.1.3 Login security and RADIUS/TACACS+ information

Table 43-3: Error messages related to login security and RADIUS/TACACS+

Message	Description
Maximum number of entries are already defined. <value1>	You are trying to add more than the allowable maximum number of entries. Delete entries that are no longer needed, and then add the entries.
	<value1>: Entry name
Port Number is duplicate between auth port and acct port.	The port numbers for auth-port and acct-port are the same.

43.1.4 SSH information

Table 43-4: SSH error messages

Message	Description
ssh: '<file path>' file open error.(<reason>)	The specified file cannot be opened.
	<file path>: The specified file <reason>: Error type
ssh: input file is bad format.	The input file format is invalid.
ssh: Public keys are a maximum of 10 entries per one user.	The maximum number of entries of public keys is 10 per user.
ssh: The number of bits of a public key is out of range.	The number of bits of a public key is out of range.
ssh: The public key is bad format.	The public key format is invalid.
ssh: The public key is nothing.	A public key cannot be found.
ssh: The public key is too long.	The public key is too long.

Message	Description
ssh: Usernames are a maximum of 20 entries.	The maximum number of entries of user names is 20.

43.1.5 Host names and DNS information

Table 43-5: Error messages related to host names and DNS

Message	Description
Same name <value> has already been set.	The same name (<value>) has already been set.

43.1.6 Device management information

Table 43-6: Device management error messages

Message	Description
Cannot change the switch model.	The device model cannot be changed.

43.1.7 Zero-touch provisioning information

Table 43-7: Zero-touch provisioning error messages

Message	Description
'system zero-touch-provisioning' and some IP configuration cannot be set together.	The "system zero-touch-provisioning" command and some IP information cannot be set at the same time. After deleting the IP information, set the "system zero-touch-provisioning" command.

43.1.8 SNMP information

Table 43-8: SNMP error messages

Message	Description
Group information exceeded 50 entries. <group name>	The number of entries specified as group information exceeded 50. Delete unnecessary entries, and then add the new one.
	<group name>: Group name
Informs is supported by only SNMPv2C.	The inform function is supported by SNMPv2C. Select SNMPv2C to use the inform function.
Invalid oid-tree. <oid tree>	The value for <oid tree> is invalid. For <oid tree>, specify an object identifier in dot notation.
	<oid tree>: Subtree information
MIB view exceeded 50 entries. <view name>	The number of MIB view entries exceeded 50. Delete unnecessary MIB view entries, and then add the new one.
	<view name>: MIB view name
RMON alarm rising threshold is less than falling threshold.	The upper threshold value is less than the lower threshold value. The upper threshold value must be equal to or larger than the lower threshold value.

Message	Description
Subtree of the same MIB view exceeded 30 entries. <view name> <oid tree>	The number of subtrees in one MIB view exceeded 30. Delete unnecessary subtrees, and then add the new one.
	<view name>: MIB view name <oid tree>: Subtree information
The number of SNMP manager entries exceeds 4.	The number of SNMP manager entries exceeded 4. Delete unnecessary SNMP manager entries, and then add the new one.

43.1.9 Advanced script information

Table 43-9: Advanced script error messages

Message	Description
The cron syntax is invalid.	The cron syntax is invalid. Check the syntax.
The event monitoring is already configured.	Event monitoring has already been set.
The file name extension is invalid.	The script file name extension is invalid. Register a file with one of the following extensions: ".py", ".pyc", and ".pyo".
The specified script id is already configured. (script id = <script id>)	The specified script ID has already been used. Delete the setting of the specified script ID or use an unused script ID for <script id>, and then try again.
	<script id>: The specified script ID
The specified sequence number is already configured. (sequence = <sequence>)	The specified action sequence number has already been used. Delete the setting of the specified action sequence number or use an unused action sequence number for <sequence>, and then try again.
	<sequence>: Action sequence number
The sysmsg syntax is invalid. (interface id = <interface id>)	The syntax of the operation message monitoring is invalid. Check the syntax.
	<interface id>: Details of the specified message type
The sysmsg syntax is invalid. (message text = <message text>)	The syntax of the operation message monitoring is invalid. Check the syntax.
	<message text>: The specified message text

43.1.10 Ethernet information

Table 43-10: Ethernet error messages

Message	Description
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.

Message	Description
Cannot attach the interface that specified cfm enable to the channel-group.	The interface for which CFM is set to enable cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete enable for CFM.
Cannot attach the interface that specified mep to the channel-group.	The interface for which MEP is set cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete MEP.
Cannot attach the interface that specified mip to the channel-group.	The interface for which MIP is set cannot participate in the port channel. To allow the specified interface to participate in the port channel, first delete MIP.
The specified port is not a PoE port.	The port specified in the parameter is not a PoE port.
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.
This command is not supported with this model.	This command or parameter is not supported on this model.

43.1.11 Link aggregation information

Table 43-11: Link aggregation error messages

Message	Description
Can not change channel-group mode.	The channel group mode cannot be changed. To change it, you must specify multiple ports to delete channel group mode, and then set it again.
Can not delete interface of channel-group because specified port status is up.	The port cannot be deleted because shutdown is not set on some ports. Use the configuration to shut down the applicable ports.
Channel-group <value1> has already been set -- <value2> cannot be set.	The same mode cannot be set under the same interface.
	<value1>: Channel group you have set <value2>: Channel group you attempted to set
Maximum number of channel-group port are already defined.	No more ports can be set. Review the number of ports for each channel group.
Relations between interface of channel-group and tpid and jumbo_frame in port configuration are inconsistent.	Information about the interface for which channel-group is set and the interface for which tpid and jumbo_frame are set is inconsistent.
The different kind of channel-group mode has already been set -- <mode> cannot be set.	The mode of the channel group which is currently set cannot be changed.
	<mode>: Mode you attempted to set
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.

43.1.12 MAC address table information

Table 43-12: MAC address table error messages

Message	Description
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	The mac-address-table static VLAN specification and the switchport configuration do not match. A VLAN set by using mac-address-table static must be specified for switchport access or switchport trunk allowed vlan of the interface that has been set.
The configuration cannot be set because the specified VLAN ID has not been configured. (VLAN ID = <vlan id>)	The specified VLAN ID has not been set. Check if the target VLAN exists.
	<vlan id>: VLAN ID

43.1.13 VLAN information

Table 43-13: VLAN error messages

Message	Description
Can not change mode from <value1> to <value2>.	The VLAN type cannot be changed to <value2> because it is already specified as <value1>. To change the VLAN type to the specified one, delete the target VLAN and then try again.
	<value1>, <value2>: VLAN type • port-based: Port VLAN • protocol-based: Protocol VLAN • mac-based: MAC VLAN
Cannot change vlan configuration referred by flow configuration.	The specified vlan configuration cannot be changed because it is specified by a filter or the QoS configuration. To change the specified vlan configuration, delete the filter or the QoS configuration set for the specified vlan configuration first.
Cannot change vlan configuration referred by QoS configuration.	The VLAN configuration cannot be changed. The port type cannot be set because the parameter that uses VLAN tunneling is set in the QoS flow list for the Ethernet interface you have set. Delete the QoS flow list for the Ethernet interface, and then specify the port type.
Cannot delete protocol referred by VLAN configuration.	You are trying to specify a protocol name to be deleted by using the "protocol" command of the VLAN. Delete the "protocol" command specification, and then delete the protocol name.
Can't delete vlan <vlan id> configuration referred by <value1> configuration.	The specified VLAN cannot be deleted because it is used by another configuration.
	<vlan id>: VLAN ID <value1>: Configuration for which VLAN is set
Can't set <value1> which is not configured to use vlan <vlan id>.	The specified VLAN ID has not been set.
	<value1>: Configuration for which VLAN ID is set <vlan id>: VLAN ID

Message	Description
Duplicate translated-tag or VLAN ID.	The specified translated ID is being used by another VLAN ID. Or, the specified VLAN ID is using another translated ID. Check the following: • Is the same translated ID specified for a different VLAN ID for all tag translation information entries of the Switch? • Is the different translated ID specified for the same VLAN ID for all tag translation information entries of the Switch? The specified translated ID specifies the VLAN ID of the trunk port. In this case, it is necessary to set the tag translation information entry of the trunk port and specify its VLAN ID.
Maximum number of TPID value which can be used is exceeded.	Too many TPID values are specified.
Maximum number which can be used is exceeded.	A maximum of 12 protocol values (ethertype value, llc value, and snap-ethertype value) are used in the entire device. No more than 12 VLANs can be set.
Mirror port and switchport are inconsistent.	The following types of ports or channel groups cannot be set as mirror ports for sessions that do not use the 802.1Q tagging function for port mirroring. • Ports other than the access port or channel groups • Ports or channel groups with tag translation enabled • Ports or channel groups belonging to VLAN • Port that is belonging to a channel group Also, The following types of ports or channel groups cannot be set as mirror ports for sessions that use the 802.1Q tagging function for port mirroring. Additionally, you cannot configure VLAN settings associated with these ports or channel groups. • Protocol port • MAC port
Not found VLAN-ID <vlan id>.	The specified VLAN ID is not set.
	<vlan id>: VLAN ID
Relations between access-list and dot1q-tunnel are inconsistent.	A tunneling port cannot be set on the device because an access list is set on the outbound side of the VLAN interface or because an access list that contains a VLAN ID as a detection condition is set on the outbound side. The tunneling port settings and the following settings cannot be specified simultaneously: • An access list that is applied to the outbound side of the VLAN interface • An access list that contains a VLAN ID as a detection condition and that is applied to the outbound side Delete the tunneling port setting or apply an access list that does not contain a VLAN ID as a detection condition to the Ethernet interface.

Message	Description
Relations between access-list and vlan mapping are inconsistent.	Tag translation cannot be set for the Ethernet interface because an access list that contains a VLAN ID as a detection condition is set on the outbound side of the Ethernet interface. Tag translation cannot be set if an access list that contains a VLAN ID as a detection condition is applied to the outbound side. Delete the tag translation setting or specify an access list that does not contain a VLAN ID as a detection condition.
	Tag translation cannot be set for the Ethernet interface because an access list is set on the outbound side of the VLAN interface. Tag translation cannot be set if an access list is applied to the outbound side. Delete the tag translation setting, or do not apply an access list to the outbound side.
Relations between mac-based and vlan-tunneling-enable are inconsistent.	MAC VLANs and VLAN tunneling cannot be set concurrently.
Relations between protocol-based and vlan-tunneling-enable are inconsistent.	A protocol VLAN and VLAN tunneling cannot be set concurrently.
Relations between vlan in dot1q configuration and default vlan are inconsistent.	The default VLAN cannot be set for the "switchport mac dot1q vlan" command (except when a native VLAN is set).
Relations between vlan in dot1q configuration and mac vlan configuration are inconsistent.	switchport mac dot1q vlan and switchport mac vlan cannot be set because they use the same VLAN.
Relations between vlan in dot1q configuration and native configuration are inconsistent.	switchport mac dot1q vlan and switchport mac native vlan cannot both be configured because they specify the same VLAN.
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	The mac-address-table static VLAN specification and the switchport configuration do not match. A VLAN set by using mac-address-table static must be specified for switchport access or switchport trunk allowed vlan of the interface that has been set.
Relations between vlan-tunneling and IP configuration are inconsistent.	VLAN tunneling information and IP information are inconsistent. When VLAN tunneling is set, IP information cannot be set.
The VLAN cannot be set because it is referred by port mirroring configuration.	The specified VLAN cannot be set because it is specified for port mirroring.
The VLAN ID cannot be deleted because it is referred by 'no mac-address-table learning'. (VLAN ID = <vlan id>)	The specified VLAN ID cannot be deleted because it is used for the MAC address learning suppression setting. Delete the configuration that refers to this configuration, and then retry the deletion.
	<vlan id>: VLAN ID
VLAN is not MAC VLAN.	A VLAN specified by switchport mac vlan is not a MAC VLAN. Specify a MAC VLAN.
VLAN is not Port VLAN.	The specified VLAN is not a port VLAN. Specify a port VLAN.
VLAN is not Protocol VLAN.	A VLAN specified by switchport protocol vlan is not a protocol VLAN. Specify a protocol VLAN.

43.1.14 Spanning Tree information

Table 43-14: Spanning Tree error messages

Message	Description
Cost is over 65535, please set up in 1 to 65535 or set pathcost method to long.	The value for cost is equal to or greater than 65535. Set the cost value from 1 to 65535 or set long for pathcost method.
Maximum number of MST instance are already defined.	The number of MST instances has already reached the maximum number. The maximum number of MST instances that can be set is 16.
Pathcost method is short, please set up in 1 to 65535 or set pathcost method to long.	short is set for pathcost method. Set the cost value from 1 to 65535 or set long for pathcost method.
Relations between PVST+ and the protocol-vlan or mac-vlan configuration are inconsistent.	PVST+ and a protocol VLAN or a MAC VLAN cannot be set concurrently.
Relations between vlan-tunneling and spanning-tree configuration are inconsistent.	The VLAN tunneling configuration does not match the Spanning Tree configuration. When a VLAN tunneling configuration is set, the Spanning Tree Protocol must be stopped.
spanning-tree: maximum number of MST instance are already defined.	The number of MST instances has already reached the maximum number. The maximum number of MST instances that can be set is 16.

43.1.15 Ring Protocol information

Table 43-15: Ring Protocol error messages

Message	Description
axrp-<ring id>-<group id>: vlan-mapping <mapping id> is already configured in another vlan-group.	The specified VLAN mapping has already been set for a VLAN group in the same ring. Either delete the VLAN mapping from another VLAN group or use another VLAN mapping.
	<ring id>: Ring ID <group id>: VLAN group ID <mapping id>: VLAN mapping ID
axrp-<ring id>: cannot configure this command to channel-group port.	A ring port cannot be set for an interface that is participating in a port channel.
	<ring id>: Ring ID
axrp-<ring id>: maximum number of ring-id are already defined.	The maximum number of ring IDs that can be used in a device is 24. No more than 24 VLANs can be set. To add a ring ID, you must first delete a registered ring ID.
	<ring id>: Ring ID
axrp-<ring id>: maximum number of ring-port are already defined.	Set two ring ports for each ring ID. To set another port as a ring port, first delete a ring port that has already been set.
	<ring id>: Ring ID

Message	Description
axrp-<ring id>: this interface is already defined as a ring port of other ring configured the same vlan-mapping.	The specified interface has already been set as a ring port of another ring to which the same VLAN mapping as the ring set by using this command is applied. Set the applicable interface as a shared link or specify another interface.
	<ring id>: Ring ID
axrp-<ring id>: vlan <vlan id> is already configured in control-vlan.	The specified VLAN has already been set in the control VLAN. Either delete the applicable VLAN from the control VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in control-vlan of other ring.	The specified VLAN has already been set in the control VLAN of another ring. Either delete the applicable VLAN from the other ring's control VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in multi-fault-detection-vlan.	The specified VLAN has already been set in the multi-fault monitoring VLAN. Either delete the applicable VLAN from the multi-fault monitoring VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in multi-fault-detection-vlan of other ring.	The specified VLAN has already been set in the multi-fault monitoring VLAN of another ring. Either delete the applicable VLAN from the other ring's multi-fault monitoring VLAN or use another VLAN.
	<ring id>: Ring ID <vlan id>: VLAN ID
axrp-<ring id>: vlan <vlan id> is already configured in 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

Message	Description
axrp-vlan-mapping-<mapping id>: vlan <vlan id> is already configured in control-vlan.	The specified VLAN has already been set in the control VLAN. Either delete the applicable VLAN from the control VLAN or use another VLAN.
	<mapping id>: VLAN mapping ID <vlan id>: VLAN ID
axrp-vlan-mapping-<mapping id>: vlan <vlan id> is already configured in multi-fault-detection-vlan.	The specified VLAN has already been set in the multi-fault monitoring VLAN. Either delete the applicable VLAN from the multi-fault monitoring VLAN or use another VLAN.
	<mapping id>: VLAN mapping ID <vlan id>: VLAN ID
axrp-vlan-mapping-<mapping id>: vlan <vlan id> is already configured in other vlan-mapping.	The specified VLAN has already been set for another mapping. Either delete the applicable VLAN from the other VLAN mapping or use another VLAN.
	<mapping id>: VLAN mapping ID <vlan id>: VLAN ID

43.1.16 IGMP snooping information

Table 43-16: IGMP snooping error messages

Message	Description
Maximum number of VLAN are already defined.	The number of VLANs that can be specified by using the IGMP snooping function is 64. No more than 64 VLANs can be set.
Relations between igmp snooping and vlan mapping are inconsistent.	VLAN mapping cannot be specified for a trunk port in a VLAN for which the IGMP snooping function is set.
Relations between igmp snooping and vlan-tunneling are inconsistent.	The IGMP snooping function and VLAN tunneling cannot be specified concurrently.
Relations between mrouter in igmp snooping configuration and channel-group configuration are inconsistent.	To specify an mrouter by using a channel group number, specify a channel group number that has already been set.
Relations between mrouter in igmp snooping configuration and switchport configuration are inconsistent.	The port or the channel group specified by an mrouter does not belong to the applicable VLAN. Specify the port or the channel group that belongs to the VLAN.

43.1.17 MLD snooping information

Table 43-17: MLD snooping error messages

Message	Description
Maximum number of VLAN are already defined.	The number of VLANs that can be specified by using the MLD snooping function is 32. No more than 32 VLANs can be set.
Relations between mld snooping and vlan mapping are inconsistent.	VLAN mapping cannot be specified for a trunk port in a VLAN for which the MLD snooping function is set.

Message	Description
Relations between mld snooping and vlan-tunneling are inconsistent.	The MLD snooping function and VLAN tunneling cannot be specified concurrently.
Relations between mrouter in mld snooping configuration and channel-group configuration are inconsistent.	To specify an mrouter by using a channel group number, specify a channel group number that has already been set.
Relations between mrouter in mld snooping configuration and switchport configuration are inconsistent.	The port or the channel group specified by an mrouter does not belong to the applicable VLAN. Specify the port or the channel group that belongs to the VLAN.

43.1.18 IPv4 communication information

Table 43-18: IPv4 communication error messages

Message	Description
An IP address is duplicated in the interface and in a route.	An address set by using IP information and an address set by using route information are the same. Set the addresses that do not duplicate one another.
Can not change IP subnetmask configuration when NTP broadcast configuration has existed.	NTP broadcast information exists. Delete the NTP broadcast information, and then change the IP subnet information.
Can not 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.
Can not delete IP configuration when NTP broadcast configuration has existed.	NTP broadcast information exists. Delete the NTP broadcast information, and then delete the IP information.
Can not delete IP configuration with ARP configuration.	ARP information exists. Delete the ARP information, and then delete the IP information.
Can not set a secondary IP address on an 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.
Cannot delete static ARP because entry assigned same IP address exists.	The static ARP entry cannot be deleted because a static ARP entry that has the same IP address exists. When a static ARP entry that has the same IP address exists, specify the static ARP entry to be deleted including the interface.
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 address is duplicate between interface and static 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.
Some IP configuration and 'system zero-touch-provisioning' cannot be set together.	The "system zero-touch-provisioning" command and some IP information cannot be set at the same time. After deleting the "system zero-touch-provisioning" command, set the IP information.

Message	Description
The following items conflict: address in the IP information and network address in the route.	There is an inconsistency between the address set with the IP information and the nexthop network address set with the route information. Set nexthop correctly.
The following items conflict: the IPv4 prefix and the mask. Non-masked bits must be zero.	1 is set for the unmasked bits of the specified prefix. Delete the address, and then set it again.
The IP configuration cannot be deleted because the route configuration has been set.	Route information exists. Delete the route information, and then delete the IP information.
The routes destined for the same destination network cannot be set.	IPv4 routes for the same destination network are set. Delete the address, and then set it again.

43.1.19 IPv6 communication information

Table 43-19: IPv6 communication error messages

Message	Description
An IPv6 address is duplicated in the interface and in a route.	An address set by using IPv6 information and an address set by using route information are the same. Set the addresses that do not duplicate one another.
Can not delete IP configuration with NDP configuration.	NDP information exists. Delete the NDP information, and then delete the IP information.
Duplicate IP address.	The same IP address has been set. Make sure that all IP addresses are unique.
Duplicate prefix.	An IP address with the same prefix has been set. Make sure that prefixes are unique.
Inconsistency has occurred in a setting of IPv6 address and NDP.	There is an inconsistency between the address prefixes of an address set in the IP information and an address set in the NDP information. Specify the address prefixes correctly.
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.
Maximum number of IP address are already defined.	No more IP addresses can be set. Check the network configuration again.
Maximum number of linklocal address are already defined.	No more link-local addresses can be set. Check the network configuration again.
Relations between ip address and local address are inconsistent.	The relation between the IP address and the local address is inconsistent. Specify an IP address that is different from the local address.
The following items conflict: address in the IPv6 information and network address in the route.	There is an inconsistency between the address set with the IPv6 information and the nexthop network address set with the route information. Set nexthop correctly.

Message	Description
The following items conflict: the IPv6 prefix and the prefixlen. Non-masked bits must be zero.	1 is set for the unmasked bits of the specified prefix. Delete the address, and then set it again.
The IPv6 configuration cannot be deleted because the route configuration has been set.	Route information exists. Delete the route information, and then delete the IPv6 information.
The MTU of the interface using IPv6 configuration must not be less than 1280.	MTU cannot be smaller than 1280 for interfaces using IPv6. Set the MTU to 1280 or higher.
The routes destined for the same destination prefix cannot be set.	IPv6 routes for the same destination network are set. Delete the address, and then set it again.

43.1.20 DHCP server function

Table 43-20: DHCP server error messages

Message	Description
<The unique key> 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.
Cannot delete the definition because referred to by <value 1>.	This configuration cannot be deleted because it is referred to by <value 1>. Delete the configuration that refers to this configuration, and then retry the deletion.
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 at '<Interface Name>'.	The interface of the specified interface name cannot be found. Specify the interface with the set interface name.
Invalid time value.	The specified time is invalid. Specify valid time.
It exceeded maximum number of IP-address pool.	The maximum number of IP address pools has been exceeded. Revise the network configuration and the excluded-address settings.
network conflicts.	The network is inconsistent. Check other network settings and host settings, and then enter a correct network.
The key name of the zone isn't found.	The key information name specified in the zone information cannot be found. Check the key information.

43.1.21 Flow detection modes/flow performance information

Table 43-21: Error messages related to flow detection modes/flow performance

Message	Description
Cannot change the flow detection mode.	The flow detection mode cannot be changed because an access list or a QoS flow list is applied to the interface. To change the flow detection mode, delete all the lists that are applied to the interface.

43.1.22 Access list information

Table 43-22: Access list error messages

Message	Description
Cannot attach this list because flow detection mode layer2-1.	If the receiving-side flow detection mode is layer2-1, the access list cannot be applied. If the flow detection mode is layer2-2, IPv4 access lists can be applied. To do so, you can use the following commands: ip access-group command
Cannot attach this list because flow detection mode layer2-2.	If the receiving-side flow detection mode is layer2-2, the access list cannot be applied. If the flow detection mode is layer2-1, MAC access lists can be applied. To do so, you can use the following commands: mac access-group command
Cannot attach this list because flow detection mode layer2-3.	If the receiving-side flow detection mode is layer2-3, the access list cannot be applied. If the flow detection mode is layer2-1, MAC access lists can be applied. To do so, you can use the following commands: mac access-group command
Over two entry as an address family cannot be set.	Another access list has already been applied. If you want to apply an access list, first delete the existing access list that has already been applied.
Relations between access-list and dot1q-tunnel are inconsistent.	A tunneling port is set on the device, so an access list cannot be set on the outbound side of the VLAN interface, or an access list that contains a VLAN ID as a detection condition cannot be set on the outbound side. The tunneling port settings and the following settings cannot be specified simultaneously: • An access list that is applied to the outbound side of the VLAN interface • An access list that contains a VLAN ID as a detection condition and that is applied to the outbound side Delete the tunneling port setting or apply an access list that does not contain a VLAN ID as a detection condition to the Ethernet interface.

Message	Description
Relations between access-list and vlan mapping are inconsistent.	An access list that contains a VLAN ID as a detection condition cannot be set on the outbound side of the Ethernet interface because tag translation is set for the Ethernet interface. Tag translation cannot be set if an access list that contains a VLAN ID as a detection condition is applied to the outbound side. Delete the tag translation setting or specify an access list that does not contain a VLAN ID as a detection condition.
	An access list cannot be set on the outbound side of the VLAN interface because tag translation is set for the Ethernet interface. Tag translation cannot be set if an access list is applied to the outbound side. Delete the tag translation setting, or do not apply an access list to the outbound side.
The maximum number of entries are exceeded.	• The number of filter entries exceeds the capacity limit. The number of used entries and available entries in the configuration file can be checked by using the "show system" operation command. • This entry cannot be set because it is not supported in flow detection mode. Change the flow detection mode to one that allows the specified entry to be set, and then try again.
This list cannot be set to the outbound of this interface because this list includes class.	This access list cannot be applied to the sending side. If Class is set as a flow detection condition in an access list, the access list cannot be applied to the sending side.
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 name has already been used for another access list. Specify a name that is not being used for another access list or specify the correct name of an applicable access list.

43.1.23 QoS information

Table 43-23: QoS error messages

Message	Description
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 layer2-2, IPv4 QoS flow lists can be applied. To do so, you can use the following commands: ip qos-flow-group command

Message	Description
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 layer2-1, the MAC QoS flow list can be applied. To do so, you can use the following commands: mac 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 layer2-1, the MAC QoS flow list can be applied. To do so, you can use the following commands: mac qos-flow-group command
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.
Specified burst size of traffic-shape rate is incorrect, or it is out of range.	The burst size specified for port bandwidth control is either incorrect or outside the specifiable range.
Specified traffic-shape rate value is incorrect, or it is out of range.	The bandwidth rate specified for port bandwidth control is either incorrect or outside the specifiable range.
The maximum number of entries are exceeded.	• The number of QoS entries exceeds the capacity limit. The number of used entries and available entries in the configuration can be checked by using the "show system" operation command. • This entry cannot be set because it is not supported in receiving-side flow detection mode. Change the receiving-side flow detection mode to one that allows the specified entry to be set, and then try again.
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.

43.1.24 Layer 2 authentication information

Table 43-24: Layer 2 authentication error messages

Message	Description
Maximum number of authentication access list are already defined.	The capacity limit of the authentication access list has been exceeded.

Message	Description
Over two entry as an address family cannot be set.	Another access list has already been applied. If you want to apply an access list, first delete the existing access list that has already been applied.
Relations between the authentication force-authorized vlan configuration and the dot1q vlan configuration are inconsistent.	When you specify a post-authentication VLAN in the configuration for forced authentication in dynamic VLAN mode, you cannot set a VLAN ID specified by the "switchport mac dot1q vlan" command.
Relations between the vlan configuration and the authentication force-authorized vlan configuration are inconsistent.	When you specify a post-authentication VLAN in the configuration for forced authentication in dynamic VLAN mode, the VLAN ID you specify must have been registered as a MAC VLAN.
The 'authentication ip access-group' cannot be set because the authentication port configuration is not set.	"authentication ip access-group" cannot be set because none of the commands listed below are set on the target port. • dot1x port-control • web-authentication port • mac-authentication port After setting one of the above commands on the target port, set it again.
The 'authentication mac access-group' cannot be set because the authentication port configuration is not set.	"authentication mac access-group" cannot be set because none of the commands listed below are set on the target port. • dot1x port-control • web-authentication port • mac-authentication port After setting one of the above commands on the target port, set it again.

43.1.25 IEEE 802.1X information

Table 43-25: IEEE 802.1X error messages

Message	Description
ChGr <channel group number>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	The mode of the "switchport mode" command, which cannot be set at the same time, is set for the channel group for which IEEE 802.1X authentication is set. The available "switchport mode" command modes are access mode, trunk mode, or MAC VLAN mode.
	<channel group number>: Channel group number
ChGr <channel group number>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	For channel groups, the ignore-eapol-start and reauthentication settings must be consistent. If reauthentication is not set, then ignore-eapol-start cannot be set. Set reauthentication first, then set ignore-eapol-start.
	<channel group number>: Channel group number
ChGr <channel group number>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	For channel groups, the ignore-eapol-start and supplicant-detection settings must be consistent. If ignore-eapol-start is set, then supplicant-detection cannot be set to disable. Conversely, if supplicant-detection is disabled, then ignore-eapol-start cannot be set.
	<channel group number>: Channel group number

Message	Description
Inconsistency is found between the dot1x configuration and the l2protocol-tunnel eap configuration.	The IEEE 802.1X configuration is inconsistent with the EAPOL forwarding configuration. The "dot1x system-auth-control" command and the "l2protocol-tunnel eap" command cannot be set simultaneously.
port <switch no.>/<nif no.>/<port no.>: Inconsistency is found between the dot1x port-control and the switchport mode configuration.	The mode of the "switchport mode" command, which cannot be set at the same time, is set for the port for which IEEE 802.1X authentication is set. The available "switchport mode" command modes are access mode, trunk mode, or MAC VLAN mode.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
port <switch no.>/<nif no.>/<port no.>: Inconsistency is found between the reauthentication and the ignore-eapol-start configuration.	For ports, the "ignore-eapol-start" and "reauthentication settings" must be consistent. If reauthentication is not set, then ignore-eapol-start cannot be set. Set reauthentication first, then set ignore-eapol-start.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
port <switch no.>/<nif no.>/<port no.>: Inconsistency is found between the supplicant-detection and the ignore-eapol-start configuration.	For port, the "ignore-eapol-start" and "supplicant-detection" settings must be consistent. If ignore-eapol-start is set, then supplicant-detection cannot be set to disable. Conversely, if supplicant-detection is disabled, then ignore-eapol-start cannot be set.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
Relations between interface in mac-address-table static configuration and dot1x port-control configuration are inconsistent.	The port or channel group used for IEEE 802.1X cannot be set as the output destination interface for static MAC address table information settings.
Relations between MLD snooping and the dot1x configuration are inconsistent.	The IEEE 802.1X configuration is inconsistent with the MLD snooping configuration. The "dot1x system-auth-control" and "MLD snooping" cannot be set simultaneously.
The authentication port configuration cannot be deleted because the 'authentication ip access-group' is set.	Cannot delete "dot1x port-control" because "authentication ip access-group" is set. Try again after deleting "authentication ip access-group".
The authentication port configuration cannot be deleted because the 'authentication mac access-group' is set.	Cannot delete "dot1x port-control" because "authentication mac access-group" is set. Try again after deleting "authentication mac access-group".
The 'switchport mode mac' and the 'dot1x multiple-host' cannot be set together on the same port.	IEEE 802.1X authentication multi-mode cannot be set for MAC VLAN ports.

43.1.26 Web authentication information

Table 43-26: Web authentication error messages

Message	Description
Duplicate IP address.	The same IP address has already been used. Specify an IP address that has not been used for an interface or local address.
Duplicate network address.	An address included in the subnet set for an interface is set as a Web authentication IP address.
Duplicate web authentication port number.	The same Web authentication port number is used more than once. Eliminate duplication of Web authentication port numbers.
Invalid max-timer . -- <value>	The maximum connection time is outside the valid range. Set a value from 10 to 1440 or the literal infinity.
	<value>: Maximum connection time for Web authentication
Invalid max-user . -- <value>	The maximum number of concurrent users is outside the valid range.
	<value>: Maximum number of concurrent users for Web authentication
Invalid vlan . -- <value>	The VLAN ID is outside the valid range. Set a value from 2 to 4094.
	<value>: VLAN ID of the VLAN after Web authentication
Invalid VLAN ID <vlan id>, not MAC VLAN	The VLAN ID you set is not the ID of a MAC VLAN.
	<vlan id>: VLAN ID of the post-authentication VLAN
Maximum number of web authentication port is exceeded.	The maximum number of Web authentication port numbers that can be added is two (in total for HTTP and HTTPS). When you add Web authentication port numbers, add a maximum of two port numbers in total for HTTP and HTTPS.
Relations between interface in mac-address-table static configuration and web-authentication port configuration are inconsistent.	The port used for Web authentication cannot be set as the output destination interface for static MAC address table information settings.
Relations between the web-authentication configuration and the VLAN mode configuration are inconsistent.	Web authentication cannot be set for a port whose VLAN mode is either tunneling mode or protocol VLAN mode.
Relations between the web-authentication logout polling configuration is inconsistent.	Processing cannot continue because there are inconsistencies between configurations for the Web authentication polling function.
The 'web-authentication port' and the MLD snooping configuration cannot be set together.	The "web-authentication port" command and MLD snooping cannot be set at the same time on the device.
The authentication port configuration cannot be deleted because the 'authentication ip access-group' is set.	Cannot delete "web-authentication port" because "authentication ip access-group" is set. Try again after deleting "authentication ip access-group".
The authentication port configuration cannot be deleted because the 'authentication mac access-group' is set.	Cannot delete "web- authentication port" because "authentication mac access-group" is set. Try again after deleting "authentication mac access-group".

43.1.27 MAC-based authentication information

Table 43-27: MAC-based authentication error messages

Message	Description
Relations between interface in mac-address-table static configuration and mac-authentication port configuration are inconsistent.	The port used for MAC-based authentication cannot be set as the output destination interface for static MAC address table information settings.
Relations between MLD snooping and mac-authentication configuration are inconsistent.	MAC-based authentication and MLD snooping cannot be used concurrently on the same device.
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.
The authentication port configuration cannot be deleted because the 'authentication ip access-group' is set.	Cannot delete "mac-authentication port" because "authentication ip access-group" is set. Try again after deleting "authentication ip access-group".
The authentication port configuration cannot be deleted because the 'authentication mac access-group' is set.	Cannot delete "mac-authentication port" because "authentication mac access-group" is set. Try again after deleting "authentication mac access-group".

43.1.28 DHCP snooping information

Table 43-28: DHCP snooping error messages

Message	Description
The VLAN target of the DHCP snooping and ARP inspection is not suitable.	The target VLAN settings for DHCP snooping and dynamic ARP inspection are invalid. The target VLAN for dynamic ARP inspection must be a VLAN subject to DHCP snooping.

43.1.29 Uplink redundancy information

Table 43-29: Uplink redundancy error messages

Message	Description
Cannot configure this command to channel-group port.	This command cannot be set for an interface participating in a port channel.
channel-group <channel group number> is invalid.	The specified channel group has already been specified for an uplink port. The same port is specified as a primary port and a secondary port.
	<channel group number>: Channel group number
Port <switch no.>/<nif no.>/<port no.> is invalid.	The specified port has already been specified for an uplink port. The same port is specified as a primary port and a secondary port.
	<switch no.>/<nif no.>/<port no.>: Switch number/NIF number/port number
Relations between flush-request transmit and mac-address-table update transmit are inconsistent.	The sending of flush control frames and sending of MAC address update frames cannot be set concurrently.

Message	Description
Relations between flush-request transmit and reset-flush-port are inconsistent.	The sending of flush control frames and port resetting cannot be set concurrently.
Relations between reset-flush-port and mac-address-table update transmit are inconsistent.	Port resetting and the sending of MAC address update frames cannot be set concurrently.
Relations between uplink redundant and ring protocol are inconsistent.	The uplink redundancy configuration is inconsistent with the Ring Protocol configuration. Uplink redundancy and the Ring Protocol cannot be configured concurrently on the same post or channel group.
Relations between uplink redundant and spanning-tree are inconsistent.	The uplink redundancy configuration is inconsistent with the Spanning Tree configuration. Uplink redundancy and the Spanning Tree Protocol cannot be configured concurrently.

43.1.30 Storm control information

Table 43-30: Storm control error messages

Message	Description
Filter-recovery-time must not be greater than recovery-time.	The flow rate limit recovery monitoring time is greater than the storm recovery monitoring time. Set the flow rate limit recovery monitoring time to a value less than or equal to the storm recovery monitoring time.

43.1.31 Port mirroring information

Table 43-31: Port mirroring error messages

Message	Description
Mirror port and monitor port are inconsistent.	Both mirror port and monitor port settings cannot be specified for the same port. When setting a channel group for a mirror port, a port that belongs to the corresponding channel group cannot be set for a monitor port.
Mirror port and switchport are inconsistent.	The following types of ports or channel groups cannot be set as mirror ports for sessions that do not use the 802.1Q tagging function for port mirroring. • Ports other than the access port or channel groups • Ports or channel groups with tag translation enabled • Ports or channel groups belonging to VLAN • Port that is belonging to a channel group Also, The following types of ports or channel groups cannot be set as mirror ports for sessions that use the 802.1Q tagging function for port mirroring. Additionally, you cannot configure VLAN settings associated with these ports or channel groups. • Protocol port • MAC port
Monitor port can specify only in one monitor session.	A monitor port can be specified only in one monitor session.

Message	Description
Relations between the session with 'encapsulation dot1q' and the session without 'encapsulation dot1q' are inconsistent within same mirror port.	Sessions that use the 802.1Q tagging function and sessions that do not use the 802.1Q tagging function cannot be set simultaneously on the same mirror port.
The number of port mirroring ethertype exceeds the maximum.	The maximum number of TPID values that can be set for port mirroring has been exceeded. When changing the TPID value, first delete all sessions that are using the 802.1Q tagging function, and then set it again.
The number of port mirroring VLAN ID exceeds the maximum.	The maximum number of VLAN ID that can be set for port mirroring has been exceeded. When changing the VLAN ID, first delete all sessions that are using the 802.1Q tagging function, and then set it again.
The port mirroring VLAN tag cannot be set because it is referred by VLAN configuration.	The VLAN tag for port mirroring cannot be set because it is specified for the VLAN configuration.

43.1.32 sFlow statistics information

Table 43-32: sFlow statistics error messages

Message	Description
Maximum number of entries are already defined.	The number of collectors that have been set exceeds the maximum. The number of collectors that have been set must not exceed four.
Only either of the following commands "sflow forward egress" or "sflow forward ingress" can be configured at a time on this device.	You can specify either sflow forward egress or sflow forward ingress for the device. To specify the sent traffic as the monitoring target, delete any sflow forward ingress specifications for other ports, and then set the command for the port to be monitored. To specify the received traffic as the monitoring target, delete any sflow forward egress specifications for other ports, and then set the command for the port to be monitored.

43.1.33 CFM information

Table 43-33: CFM error messages

Message	Description
Cannot change cfm domain direction.	The MEP direction that is set in a domain cannot be changed.
Cannot change cfm mep direction.	The MEP direction cannot be changed.
Cannot configure cfm enable to channel-group port.	CFM of an interface participating in a port channel cannot be enabled.
Cannot configure cfm mep to channel-group port.	An MEP cannot be set for an interface that is participating in a port channel.
Cannot configure cfm mip to channel-group port.	An MIP cannot be set for an interface that is participating in a port channel.

Message	Description
Domain level <level> is set with a value less than cfm mep.	A value equal to or smaller than the value set for the MEP is specified for the specified domain level.
	<level>: Domain level
Domain level <level> is set with values more than cfm mip.	A value equal to or greater than the value set for MIP is specified for the specified domain level.
	<level>: Domain level
MA <no.> is already configured in cfm domain.	The specified MA identification number is already being used by another domain.
	<no.>: MA identification number
MA name <name> is already configured in cfm domain.	The specified MA name is already set in the same domain.
	<name>: MA name
Maximum number of cfm mep are already defined.	The number of MEP settings exceeds the maximum. Delete unnecessary MEP settings.
Maximum number of cfm mip are already defined.	The number of MIP settings exceeds the maximum. Delete unnecessary MIP settings.
MEP ID <mepid> is already configured in cfm mep.	The specified MEP ID has already been set for another MEP.
	<mepid>: MEP ID
Not found VLAN ID <vlan id> in MA.	The specified VLAN ID does not exist. Specify a VLAN ID that has already been set in the MA.
	<vlan id>: VLAN ID
VLAN ID <vlan id> is already configured in MA name.	The specified VLAN ID is already being used by another MA name.
	<vlan id>: VLAN ID